Sumário

Generalidades

Nos tempos da rede mundial e dos riscos de segurança massivos resultantes, o tópico *Proteção contra vírus* não diz mais respeito somente aos especialistas em TI. Isso precisa muito mais ser considerado no escopo de um abrangente gerenciamento de riscos, por toda a empresa, no nível de gerenciamento mais alto. Uma queda da rede de computadores, causada por vírus, atinge uma empresa em seu ponto mais sensível. As consequências: A parada de sistemas indispensáveis, perda de dados relevantes ao sucesso e a queda de importantes canais de comunicação. Vírus de computadores podem causar danos a uma empresa, dos quais ela nunca mais se recupera! A *G Data* oferece a proteção contra vírus de alta capacidade para toda a sua rede. O desempenho de segurança líder de mercado dos produtos da *G Data* tem sido, há anos, premiado em inúmeros testes com uma nota invejável. *G Data EndpointProtection* aposta, de forma consequente na configuração e administração central, assim como na maior automatização possível. Todos os clientes, estação de trabalho, notebook ou servidor de arquivos são gerenciados centralmente. Todos os processos do cliente são executados em segundo plano, de forma transparente. Atualizações automáticas da Internet possibilitam, em casos de ataques de vírus graves, um tempo de reação extremamente curto e o firewall cliente premiado complementam a proteção completa. O controle central com o *G Data ManagementServer* possibilita a instalação, configurações, atualizações, controle remoto e automático para toda a rede. Isso alivia o administrador do sistema e economiza tempo e custos e com o Gerenciador de políticas obtém-se, além disso, a perfeita segurança no trato com PCs empresariais..

PremiumHotline

A instalação e utilização do *G Data Software* é normalmente intuitiva e descomplicada. Se ocorrer um problema em algum momento, basta entrar em contato com o***Suporte técnico G Data*** através da Internet.

www.gdatasoftware.com.br

Serviço antivírus emergencial

Se constatar um novo vírus ou um fenômeno desconhecido, envie-nos por gentileza, em todos os casos, esse arquivo através da função de quarentena do *G Data Software*. Nós analisaremos o vírus e disponibilizaremos um antídoto o mais rápido possível. Naturalmente, trataremos os seus dados de forma altamente confidencial e discreta.

? O endereço de resposta para arquivos que foram reparados pelo Serviço emergencial antivírus pode ser definido na área ***Configurações de e-mail*** .

Antes da instalação

No caso de uma grave suspeita de vírus, realize primeiro um ***BootScan*** nos computadores afetados.

- Em seguida, instale o ***ManagementServer*** no seu servidor. Na instalação do ManagementServers o ***Administrador*** será instalado automaticamente no servidor. Com esse programa, será possível controlar o ManagementServer a partir do computador servidor. Para garantir a proteção ideal, o computador deverá estar sempre acessível (ativado) e dispor de um acesso à Internet para o carregamento automático das assinaturas de vírus. Ou seja, o ManagementServer não precisa, imprescindivelmente estar instalado no seu servidor de arquivos principal.
- Execute agora o ***Registro on-line***. Sem o registro online não é possível executar a atualização dos bancos de dados de vírus através da Internet.
- Na primeira inicialização do Administrator no servidor o ***Assistente de instalação***é iniciado. Através dele é possível instalar diretamente o ***software cliente*** nos clientes desejados na rede sem executar diretamente essa instalação em todos os clientes individualmente.
- Se ocorrerem problemas com a ***Instalação remota*** dos clientes, naturalmente o software cliente poderá ser instalado manualmente ou de forma semi-automática nos clientes. Para que o seu servidor seja protegido de infecções de vírus, o software cliente deverá ser também instalado no seu servidor.
- Agora será possível executar profilaxias e combates a vírus, assim como atualizações na Internet do *software G Data Cliente do servidor* de forma simples e centralizada, utilizando a ***Sentinela G Data*** para os controles correntes ou definir tarefas de verificação que investigam a sua rede constantemente procurando por infecções de vírus.
- Se tiver que alguma vez solucionar problemas *no local* poderá instalar simples e rapidamente o software Administrator em cada cliente e terá acesso de lá ao ManagementServer.

Requisitos do sistema

O *sistema G Data* utiliza o ***protocolo TCP/IP*** e aproveita esse tanto para a comunicação com computadores cliente e servidor entre si, como também para a conexão online ao *G Data UpdateServer*. Os seguintes pré-requisitos mínimos são exigidos em clientes ou servidor:

- ***G Data ManagementServer***: PC com no mín. 128 MB RAM, acesso à Internet. Sistemas operacionais possíveis: Windows 7, Windows Vista, Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 (preferencialmente as versões servidores, também a x64 Edition),
- ***G Data Clientes***: PC com no mín. 256 MB RAM. Sistemas operacionais possíveis: Windows 7, Windows Vista, Windows XP, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 (também a x64 Edition),

? Para ***computadores Linux*** que funcionam como Servidor de arquivos e disponibilizam liberações do Windows aos diversos clientes (através do ***protocolo SMB***), pode ser manualmente instalado um módulo que controla o acesso às liberações e executa uma verificação nos arquivos a cada acesso, de forma que nenhum malware de ***servidor Samba*** possa acessar os clientes Windows (e vice-versa).

BootScan

O ***BootScan*** ajuda a combater vírus que se aninharam em seu computador antes da instalação do software antivírus e que, possivelmente, podem impedir a instalação do ***G Data Software***. Para isto, existe uma versão especial do programa do ***G Data Software***, que pode ser executada já antes da inicialização do Windows.

? ***O que faço quando meu computador não faz o boot a partir do CD-ROM?*** Se não for possível o boot a partir do CD/DVD-ROM, pode ser que essa opção precise primeiro ser ativada. Isso é feito na ***BIOS***, um sistema que é inicializado automaticamente antes do sistema operacional Windows. Para fazer alterações aqui, execute as seguintes etapas:

1. Desligue o seu computador.
2. Reinicialize o computador. Normalmente, você consegue acesso à configuração da BIOS, ao iniciar (= Boot) o computador você pressionar a tecla ***Del*** (algumas vezes também a tecla ***F2*** ou ***F10***).

3. A forma de alteração individual na configuração da BIOS é diferente de computador para computador. Leia para isto, a documentação do seu computador. Em resumo, a sequência do boot deve ser ***CD/DVD-ROM:, C:*** ou seja, a unidade de CD/DVD-ROM será o ***1st Boot Device*** e a partição do disco rígido, com o seu sistema operacional Windows, será o ***2nd Boot Device***.
4. Salve as alterações e reinicie o seu computador. Agora o computador estará pronto para um BootScan.

Proceda da seguinte forma no ***BootScan***:

1a ***BootScan com o CD do programa***: Utilize o ***CD do programa G Data*** e dê o boot no seu computador utilizando-o. - Insira o ***CD do G Data Software*** na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

1b ***BootScan com o software G Data, descarregado da Internet***: Através do registro **Criar CD de boot G Data** no ***grupo de programas G Data Software*** você grava um novo CD de Boot. - Insira o seu próprio CD gravado na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

Após a primeira etapa o BootScan para as três variações tem o mesmo procedimento:

2 Reinicialize o computador. O menu de inicialização do ***G Data BootScan aparece.***.

3 Com as setas, selecione a opção **CD de boot G Data** e confirme a seleção com **Enter**. Um sistema operacional Linux será iniciado pelo CD, e aparecerá uma ***versão especial da G Data*** para BootScans.

? Se tiver problemas com a visualização da interface do programa, reinicialize o seu computador e selecione a opção **CD de boot G Data – Alternativo**.

4 O programa agora irá sugerir a atualização das proteções antivírus (também chamadas de ***assinaturas de vírus***).

5 Clique aqui em **Sim** e execute a atualização. Assim que os dados tiverem sido atualizados na Internet, aparecerá o aviso ***Atualização concluída***. Saia agora da tela de atualização clicando no botão **Fechar**.

? A ***atualização automática na Internet*** é disponibilizada quando for utilizado um ***roteador*** que atribua endereços IP automaticamente (***DHCP***). Se não for possível a atualização na Internet, o ***BootScan*** poderá ser executado também com as assinaturas de vírus antigas. No entanto, neste caso, após a instalação do ***G Data Software***, você deverá executar o mais rápido possível um novo BootScan com dados atualizados.

6 Agora você verá a interface do programa. Clique no registro **Verificar computador** e o seu computador será agora verificado quanto à existência de vírus e softwares maliciosos. Este processo pode levar uma hora ou mais, dependendo do tipo de computador e tamanho do disco rígido.

7 Se o ***G Data Software*** encontrar vírus, remova-os com a ajuda da opção sugerida no programa. Após a remoção bem-sucedida do vírus, o arquivo original ficará novamente disponível.

8 Após a conclusão da verificação de vírus, saia do sistema clicando no botão ***Finalizar***e, em seguida, selecionando **Reiniciar** .

O botão ***Finalizar*** está localizado na parte inferior direita da interface do programa Linux.

9 Remova o ***CD G Data Software*** da unidade, assim que a unidade abrir.

10 Desligue novamente o seu computador e o reinicie. Agora, o seu computador inicializará novamente com o sistema operacional Windows padrão e você terá a garantia de poder instalar o ***G Data software*** normal em um sistema sem vírus.

Instalação

A instalação da *versão G Data Windows* é extremamente fácil. Basta iniciar o Windows e colocar o *CD-ROM G Data* na sua unidade de CD-ROM. Uma janela de instalação é aberta automaticamente.

? Se não tiver ativado o ***recurso de inicialização automática de sua unidade de CD-ROM*** , o *G Data Software* não pode iniciar automaticamente o processo de instalação. Assim, clique no ***menu Iniciar*** do Windows, em ***Executar***, na janela que aparece, digite ***e:\setup.exe*** e clique em ***OK***. Dessa forma, a tela de inicialização também é aberta para a*instalação do G Data Software*. O registro ***e:*** indica a letra da unidade de sua unidade de CD-ROM. Se tiver registrado a sua unidade de CD-ROM em uma outra letra, insira, ao invés de ***e:*** a letra da unidade correspondente.

Feche todos os outros programas antes de começar a instalação do *G Data Software*. Se forem abertos programas que acessem os dados necessários para a instalação do *G Data Software*, podem ocorrer erros de funcionamento ou uma interrupção.

- **Instalar**: Com um clique nesse botão, você inicia a instalação do *G Data Software* em seu computador
- **Procurar**: Através do Windows Explorer você poderá visualizar os diretórios do CD do Software.
- **Cancelar**: Através desse registro, você pode fechar a tela de inicialização automática sem executar uma ação.

Após ter pressionado o botão **Instalar**, aparecerá uma tela na qual é possível selecionar quais *componentes do G Data Software* você deseja instalar. Estão disponíveis as seguintes possibilidades de instalação:

- **G Data ManagementServer**: Primeiro, o ***ManagementServer*** deve ser instalado no computador onde você deseja usar o servidor antivírus. O ManagementServer é o coração da *Arquitetura G Data*: Ele administra os clientes, invoca novas atualizações de software e assinaturas de vírus automaticamente do *G Data UpdateServer* , além de controlar a tecnologia de vírus na rede. Com a instalação do ManagementServer, automaticamente é aberto, no servidor, o ***software Administrator*** , com o qual você pode controlar o ManagementServer.

- **G Data Administrador**: O ***Administrator*** é o software de controle para o ManagementServer, o qual, controlado centralmente pelo administrador do sistema, protege toda a rede. O Administrator pode ser iniciado protegido por senha, a partir de qualquer computador com Windows.
- **G Data Client**: O ***software cliente*** disponibiliza a proteção antivírus para os clientes e executa as tarefas do ManagementServer sem a interface do usuário em segundo plano. A instalação do software cliente ocorre, normalmente, centralizando todos os clientes através do Administrator.
- **Criação do CD de boot**: Com a ajuda do assistente do CD de Boot, é possível criar um CD com capacidade de Boot para verificação básica de seu computador, antes da inicialização do sistema operacional Windows. Para isso, são utilizadas as assinaturas de vírus atuais. Com a criação de um CD de boot, é possível executar um ***BootScan*** mesmo sem o *CD do software G Data* original. Para isto, leia também o capítulo ***BootScan***.
- **G Data WebAdministrator**: O ***WebAdministrator*** é um software de controle, baseado na web, para o ManagementServer. Ele pode ser iniciado por meio de um navegador da Internet.
- **Firewall**: Com o ***Firewall*** , é possível proteger os clientes adicionalmente com um firewall. Quando você instala manualmente o firewall no respetivo cliente, o *software G Data Client* deverá ter sido rodado nesse cliente antes, porque ele regula a comunicação do firewall com o ManagementServer.

? Observações e informações sobre o que deve ser observado sobre a instalação dos respetivos módulos podem ser encontradas no capítulo do respetivo componente de software.

G Data ManagementServer

O ***ManagementServer*** é o coração da *Arquitetura G Data*: Ele administra os clientes, invoca novas atualizações de software e assinaturas de vídeo automaticamente do *G Data UpdateServer* e controla a tecnologia de vírus na rede. Para comunicação com os clientes, o ManagementServer utiliza o ***TCP/IP***. Para ***Clientes*** offline, as tarefas são automaticamente reunidas e sincronizadas na próxima sessão online. O ManagementServer dispõe de uma pasta central de ***Quarentena***, na qual é possível, como opção, criptografar arquivos suspeitos e protegê-los, exclui-los, desinfetá-los ou, eventualmente, encaminhar ao ***Serviço emergencial antivírus***. O ManagementServer é controlado através do ***software Administrator***.

? Ao finalizar o software Administrator, você não fecha o ManagementServer. Esse permanece ativo em segundo plano e controla os processos que não foram definidos para os clientes.

Instalação do ManagementServer

Insira o *CD-ROM G Data-CD* e pressione o botão **Instalar**. Em seguida, selecione o componente **G Data ManagementServer** com um clique no botão ao lado.

Tela de saudação

Na tela de saudação a seguir, você é informado que está prestes a instalar o ManagementServer em seu sistema. Feche, o mais tardar agora, todos os aplicativos abertos em seu sistema Windows, porque esses poderão causar problemas na instalação. Clique em **Continuar**, para prosseguir com a instalação.

Acordo de licença

Leia agora, por gentileza, o acordo de licença para uso deste software, selecione **Estou de acordo com as condições deste acordo de licença** e clique em **Continuar**, quando concordar com os acordos deste formulário.

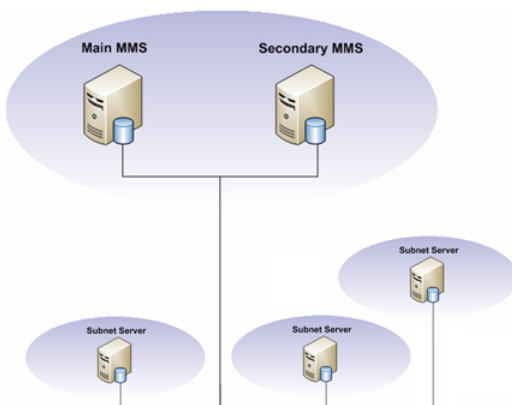
Pasta destino

A tela seguinte possibilita a seleção do local no qual os dados do ManagementServer deverão ser salvos. Se desejar selecionar uma pasta de destino individual, você tem a possibilidade de, através do botão **Alterar** , abrir uma visualização de diretório, na qual você pode selecionar um outro diretório, ou criar um novo.

Selecionar tipo de servidor

Na seleção dos tipos de servidores, você tem as seguintes opções:

- **Instalar um servidor principal**: É fundamental definir o *G Data ManagementServer* como ***servidor principal*** (***Main-MMS***). O servidor central representa a instância de configuração e administração central da arquitetura de proteção contra vírus baseada na rede. Os computadores a serem protegidos são fornecidos através do ManagementServer com as atualizações de assinatura de vírus e atualizações de programas mais atuais. Além disso, todas as configurações específicas do cliente são feitas de forma central no ManagementServer.
- **Instalar um servidor secundário**: Na utilização de um ***banco de dados SQL***, é possível operar um ***segundo servidor*** (***MMS secundário***) que utiliza o mesmo banco de dados que o servidor principal. Caso o ***servidor principal*** não esteja acessível por uma hora ou mais, os clientes serão conectados automaticamente com o MMS secundário e carregarão as atualizações de assinaturas do mesmo. A troca de volta para o servidor principal ocorre assim que esse estiver novamente disponível. Ambos os servidores carregam as atualizações de assinaturas de forma independente entre si.
- **Instalar servidor de subrede**: Em grandes redes, é sensato utilizar o *G Data ManagementServer* também como ***servidor de subrede***. O servidor de subrede serve para aliviar a carga do tráfego da rede entre clientes e o MMS principal. Eles podem ser utilizados em unidades de subrede e administram, lá, os clientes a ele atribuídos. O servidor de subrede é totalmente operacional, mesmo quando o ManagementServer principal ou secundário não puder ser acessado.

De forma esquemática, uma ***estrutura de tipos de servidores*** seria em grandes redes assim: Servidores de subrede vinculam clientes individuais ou grupos de clientes e os repassam ao servidor principal. Esse terá o suporte de um servidor secundário que funcionará como backup, no caso de uma queda do servidor principal.

Servidor do banco de dados

Selecione agora um servidor de banco de dados para instalar. Você tem a possibilidade de utilizar um ***Servidor SQL*** existente, ***Microsoft SQL-Express*** ou um ***banco de dados integrado*** (p.ex., para redes menores).

> **?** Um sistema operacional de servidor não é forçosamente necessário. A opção de SQL é adequada principalmente a grandes redes com uma quantidade > 50 clientes.

Nome do computador

Verifique agora o ***Nome do seu computador***, no qual você instalou o ManagementServer. Esse computador deverá poder ser contactado através do nome do cliente, na rede, informado aqui. Se o nome correto não for exibido, altere os dados, de acordo, em **Nome**.

Começo da instalação

Agora será feita a instalação do ManagementServer. A instalação será iniciada com uma tela inicial. Clique em **Instalar**.

Registro on-line

O mais tardar antes da execução de uma ***Atualização na Internet*** é preciso registrar-se no *G Data UpdateServer*, a fim de obter seus dados de acesso. Para isso, é possível executar o registro diretamente durante a instalação ou posteriormente, abrindo a função **Atualização na Internet** em ***Iniciar > Programas > G Data ManagementServer***. Pressione aqui o botão **Registro on-line**. Em seguida, você será solicitado a informar seus dados de cliente e o número do registro.

? O ***Número de registro*** pode ser encontrado na contra-capa do manual de utilização. Se tiver comprado o software on-line, você receberá, após o pedido, o número de registro em um e-mail específico.

? Observe também que, naturalmente, é preciso existir uma ***Conexão à Internet*** através de linha normal ou por discagem, ou uma deverá ser estabelecida.

Informe o número do registro sequencialmente sem dígitos separadores nos cinco campos de entrada correspondentes. Preencha também todos os outros campos de entrada corretamente, porque o registro online só pode ocorrer com os dados aqui solicitados. Imediatamente após o registro online, você obterá em uma caixa de informações, seu nome de usuário e sua senha.

? ***Atenção***: Anote ***nome de usuário*** e ***senha*** em local seguro para que os mesmos estejam à disposição em caso de uma possível reconfiguração de seu computador.

? O *G Data Software* aplica esses dados automaticamente no formulário de atualização. Agora você tem a possibilidade de executar uma atualização na Internet.

? O botão ***Atualização na Internet*** pode ser executado diretamente a partir da interface do administrador e até mesmo ser automatizado de acordo com esquemas temporais livremente variáveis.

Configuração do tipo de banco de dados

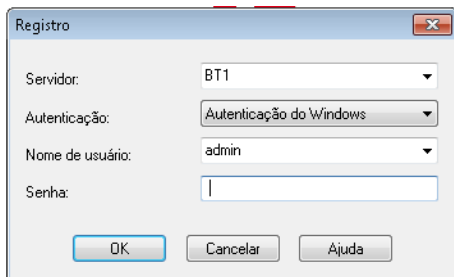
Essa etapa de configuração só ocorre quando você reinstala o ManagementServer ou quando um ***Banco de Dados SQL*** estiver pré-instalado no computador. Normalmente basta fechar essa caixa de informações clicando no botão **Fechar**-.

Conclusão da instalação

Após a instalação e após cada reinicialização do computador, o ManagementServer será agora inicializado automaticamente. Para efetuar alterações no ManagementServer, você pode selecionar, em ***Iniciar > (Todos os) Programas > G Data ManagementServer***, o registro ***G Data Administrador*** e, dessa forma, iniciar o Administrationstool para o ManagementServer.

G Data Administrador

O ***Administrator*** é o software de controle para o ManagementServer, o qual, controlado centralmente pelo administrador do sistema, protege toda a rede. O Administrator pode ser iniciado protegido por senha, a partir de qualquer computador com Windows. Como tarefas controladas remotamente, são possíveis todas as condições imagináveis de verificadores de vírus, como instalações, atualizações de software e de assinaturas de vírus (imediatas ou periódicas), funções de sentinela e alterações de configurações por toda a empresa. A ferramenta Administrator pode ser aberta para controle do ManagementServers com um clique no registro ***G Data Administrator*** no grupo de programas ***Iniciar > (Todos os) Programas > G Data ManagementServer*** no menu Iniciar.

Instalação do Administrator

Na instalação do ***ManagementServer*** , será instalado automaticamente, no mesmo computador (ou seja, o computador que você deseja utilizar como ***Servidor***), o ***Administrator***. Portanto, a instalação do Administrator não precisa ser executada adicionalmente. A instalação do Administrator pode, no entanto (independente da instalação no servidor), também ser feita em todos os computadores cliente. Dessa forma, o ManagementServer pode também ser controlado de forma descentralizada. Para a instalação do Administrator em um computador cliente, insira o *CD-ROM G Data* na unidade de CD-ROM do computador cliente e pressione o botão **Instalar**. Em seguida, selecione o componente **G Data Administrator** com um clique no botão ao lado.

Na tela de saudação a seguir, você será informado de que está prestes a instalar o Administrator em seu sistema. Feche, o mais tardar agora, todos os aplicativos abertos em seu sistema Windows, porque esses poderão causar problemas na instalação. Clique em **Continuar**, para proceder com a instalação e siga as etapas, guiado pelo Assistente de instalação. Após a instalação, você pode, em ***Iniciar > (Todos os) Programas > G Data ManagementServer***, selecionar o registro ***G Data Administrator*** e dessa forma iniciar a Administrationstool para o ManagementServer.

Registro

Ao iniciar o administrador, você será solicitado a informar **Servidor**, **Autenticação**, **nome de usuário** e **senha**.

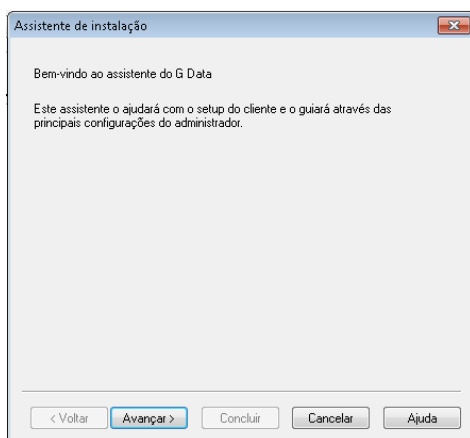
No campo **Servidor**, insira o nome do computador no qual o ManagementServer foi instalado.

Selecione, em seguida, a sua **Autenticação**.

- **Autenticação do Windows**: Se optar por esse tipo de autenticação, poderá fazer o login com o nome de usuário e senha do seu acesso como administrador nesse computador, ou seja, a ***Conta de usuário do Windows***.

- **Autenticação integrada**: Com a autenticação integrada, é possível a você, como administrador, conceder a outros pessoas o acesso ao *G Data Administrator*. Por exemplo, uma conta pode ser configurada, que contenha apenas direitos de leitura. Essas contas adicionais podem ser criadas e administradas através da função ***Administração do usuário*** .

Primeira inicialização do programa (Assistente de instalação)

Na primeira inicialização do Administrator, será automaticamente aberto o ***Assistente de instalação***. Ele ajuda na instalação do cliente e o conduz através de todas as configurações essenciais. O assistente também pode ser iniciado após a primeira instalação, através do comando **Assistente de instalação** no menu **Arquivo**, a qualquer momento.

Ativar

Primeiro, todos os clientes que tiverem que ser monitorados pelo *G Data Software* devem ser ativados. Marque os computadores na lista e, em seguida, pressione o botão **Ativar**. Eventualmente, alguns computadores podem não estar contidos na lista (p.ex., quando não tiverem sido ligados a algum tempo ou a liberação de arquivos ou impressão não tiver sido configurada). Para a ativação desses clientes, é possível inserir o nome no campo de entrada **Computador** e pressionar o botão **Ativar** ao lado do campo de entrada. O computador será inserido na lista. Pressione **Continuar**, após ter ativado todos os clientes.

Instalar

No diálogo a seguir, a marcação é predefinida automaticamente em **Instalar software cliente automaticamente no computador ativado**. Quando preferir instalar manualmente o software nos computadores cliente, remova a marcação aqui.

Configurações padrão

No diálogo a seguir, você pode alterar as configurações padrão para sentinela, além de proteção antivírus e do cliente. As configurações padrão são selecionadas de tal forma que podem ser utilizadas sem alterações, diretamente, para a maioria das redes. Se essas configurações não forem exatamente ideais para sua rede, essas poderão ser alteradas posteriormente através das respetivas áreas de trabalho do Administrator. Explicações detalhadas sobre as opções configuráveis podem ser encontradas nas explicações sobre a área de tarefas **Configurações**.

Atualização na Internet

O ManagementServer pode carregar novas assinaturas de vírus e arquivos de programa através da Internet. Para que esse processo possa ocorrer automaticamente, os registros e eventualmente a discagem precisam ser automatizados. Insira aqui, primeiro, os ***Dados de acesso*** recebidos no registro online. Uma descrição detalhada para o planejamento de intervalos de atualização e a execução de configurações básicas podem ser encontradas no capítulo ***Atualização na Internet***. Naturalmente a atualização na Internet pode ser automatizada a qualquer momento posterior, através da interface do programa Administrator.

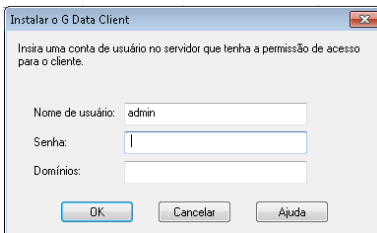
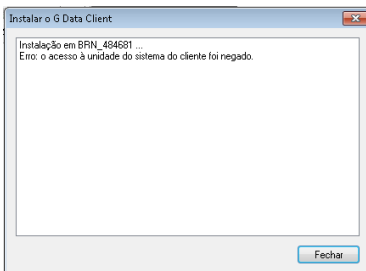
Configurações de e-mail

O ManagementServer pode enviar arquivos potencialmente infectados para verificação ao ***Serviço antivírus emergencial***. Para que isso possa ocorrer através da pressão em um botão, é preciso informar o nome do ***Servidor de e-mail***, o ***Número da porta*** (***SMTP***) e o ***endereço do remetente*** . As respostas do ***Serviço emergencial antivírus*** serão enviadas para esse endereço de e-mail.

Notificação por e-mail

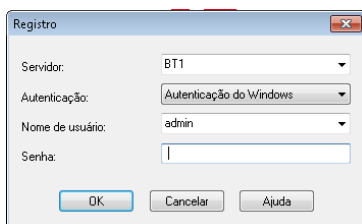
O ManagementServer pode informar, ao administrador da rede por e-mail, quando um vírus for encontrado em um dos clientes. Para isso, informe o endereço de e-mail do destinatário do aviso de vírus. Através de **Limitação de quantidade** , é possível evitar que sua caixa postal seja *inundada* de notificações em caso de uma infecção em massa. Pressione **Concluir** para finalizar o assistente.

Instalação automática do software cliente

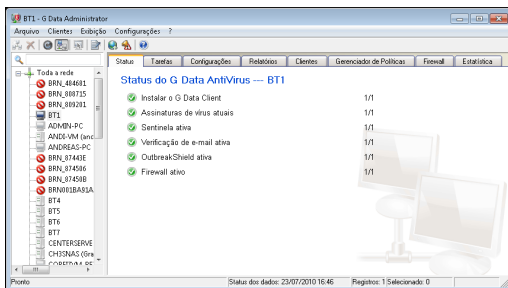
Quando você informa que o software cliente deve ser instalado automaticamente, será solicitado a inserir uma conta de usuário no servidor que tenha permissão de acesso para o cliente.

Após confirmação do diálogo, o ManagementServer tenta instalar o software cliente em computadores ativados. Uma tela informativa avisa sobre o andamento da instalação e eventuais problemas.

? Se ocorrerem problemas na ***Instalação remota*** do *G Data Client* através do Administrator, existe a possibilidade de instalar o software cliente manualmente ou de forma semi-automática, nos computadores cliente. Para isto, leia também o capítulo ***Instalar o G Data Client***.

? Também é possível instalar um software cliente especial em ***clientes Linux*** na rede. Para isto, leia o capítulo ***Leia para isso o capítulo Software cliente em computadores Linux*** no anexo desta documentação.

Outras inicializações do programa (senha de acesso)

A ferramenta Administrator pode ser aberta para controle do ManagementServers com um clique no registro ***G Data Administrator*** no grupo de programas ***Iniciar > Programas > G Data ManagementServer*** no menu Iniciar. Na inicialização do Administrator você será perguntado pelo servidor e senha. No campo **Servidor**, insira o nome do computador no qual o ManagementServer foi instalado.

A interface do programa será aberta. Suas funções serão explicadas nos próximos capítulos.

Estrutura do programa Administrator

A interface do Administrator é subdividida da seguinte forma:

A ***Área de Seleção de clientes, encontrada à esquerda,*** mostra a estrutura hierárquica do computador monitorado. À direita dessa, através de guias, é possível alternar para a respetiva ***Área de tarefas***. O conteúdo da área de tarefas está normalmente relacionado ao computador marcado na área de seleção de clientes ou no grupo de clientes selecionado. Acima dessa coluna, você encontra uma ***Barra de menu*** e ***Barra de ferramentas*** para funções globais, que pode ser utilizada em todas as áreas de tarefas.

? Na administração de ***Clientes Linux***, que atuam como ***servidor Samba***, existem funções que, p.ex, contêm o trato com e-mails, bloqueios, que nesse contexto de um servidor de arquivo não são necessárias. As funções que não são configuráveis para os clientes Linux são marcadas por um ponto vermelho à frente da respetiva função.

Barra de menu

A barra de menu contém funções globais que podem ser utilizadas em todas as áreas de tarefas. Para isso, você tem uma subdivisão nas seguintes áreas:

- **Arquivo**
- **Clientes**
- **Exibir**
- **Tarefas** (somente na área de tarefas **Tarefas**)
- **Relatórios** (somente na área de tarefas **Relatórios**)
- **Configurações do cliente** (somente na área de tarefas **Clientes**)
- **Configurações do firewall** (somente na área de tarefas **Firewall**)
- **Configurações**
- ***? (Ajuda)***

Arquivo

No menu Arquivo, estão disponíveis as funções básicas de administração e impressão, assim como o ***Assistente de instalação*** .

Assistente de instalação

Com o assistente de configuração, é possível, em um processo com suporte ao usuário, selecionar os clientes de sua rede e ativá-los para aqueles clientes que você deseja que sejam controlados através do *G Data Software*. O assistente de instalação é explicado detalhadamente no capítulo ***Primeira inicialização do programa (Assistente de instalação)*** .

Exibir registro

Através do ***Arquivo de registro***, você tem uma rápida visão global sobre as últimas ações do *G Data Software*. Aqui são exibidas todas as informações relevantes. A exibição do registro pode ser filtrada através das seguintes áreas de configuração:

- **Exibição do registro**: Defina aqui se deseja ver um registro dos procedimentos do cliente ou servidor.
- **Computador/Grupo**: Aqui é possível definir se deseja ver um registro de todos os clientes ou grupos ou apenas áreas individuais.
- **Procedimento**: Defina aqui se deseja ver todas as informações relacionadas ao registro ou apenas mensagens sobre um determinado tópico.
- **Período**: Aqui é possível definir o período de/até para os quais as informações de registro deverão estar disponíveis.

O campo **Atualizar** serve para relacionar processos que surgem enquanto a visualização do registro está aberta. Através de **Fechar**, é fechada a janela do arquivo de registro; além disso, você pode imprimir o registro ou ***imprimir*** e ***exportar*** uma área selecionada do registro (em formato XML). Todos os processos aparecem primeiro em uma ordem cronológica e podem ser classificados através de um simples clique na respetiva designação da coluna, por determinados critérios. A coluna, de acordo com a qual a classificação atual é feita, é marcada através de uma pequena seta.

Administração do usuário

Como administrador do sistema, você pode atribuir o acesso a outros usuários para a interface do Administrator. Para isso, clique no botão **Novo** e, em seguida, insira o nome do usuário, as **permissões** desse usuário (**Leitura/Gravação** ou **somente leitura**), defina o **Tipo de conta** (**Login integrado**, **usuário do Windows**, **Grupo de usuários do Windows**) e atribua uma**Senha** a esse usuário.

Gerenciar o servidor

Através da Administração do servidor, é possível atribuir, aos ***Clientes , servidores de subrede*** individuais, que vinculam a comunicação desses clientes com o ***servidor principal*** e otimizam, assim, a utilização da rede. Através desse menu, é possível instalar o servidor de subrede. Através do botão **Atribuir clientes**, você pode atribuir, aos clientes existentes, os servidores de subrede definidos.

? A atribuição dos clientes aos servidores de subrede independe do agrupamento de clientes em relação às verificações de vírus. Clientes de diferentes servidores de subrede podem serem agrupados naturalmente em um grupo para ***controle de vírus*** e tarefas de verificação.

Sincronização do servidor de subrede

Para possibilitar eventuais alterações também fora dos intervalos de comunicação habituais do servidor e servidor da subrede, é possível executar a sincronização deste também manualmente.

Modelos de impressão

Aqui é possível efetuar abrangentes configurações para a impressão de funções de registro e estatísticas, além de salvá-las em modelos utilizáveis de forma independente uns dos outros.

? Dependendo da ***área de tarefas selecionada*** você obterá diferentes diálogos de opção e possibilidades de configuração. Nem todas as áreas de tarefa têm opções de impressão disponíveis.

Visualizar página

Neste menu, é possível definir detalhes e dados que deseja imprimir. Na janela de opções que aparece, é possível selecionar os elementos desejados para a impressão e, através de **OK**, será direcionado para a visualização de página que exibirá uma prévia na tela da impressão.

? Dependendo da ***área de tarefas selecionada*** você obterá diferentes diálogos de opção e possibilidades de configuração. Nem todas as áreas de tarefa têm opções de impressão disponíveis.

Imprimir

Através desta função, você inicia o processo de impressão de configurações do cliente ou relatórios. Na janela que aparece, é possível definir os detalhes e as áreas das configurações do cliente que deseja imprimir.

? Dependendo da ***área de tarefas selecionada*** você obterá diferentes diálogos de opção e possibilidades de configuração. Nem todas as áreas de tarefa têm opções de impressão disponíveis.

Finalizar

Através desta função, você finaliza o Administrator. Naturalmente, o monitoramento de sua rede é feito de acordo com os dados que você passou para o ManagementServer e continua quando o Administrator não está aberto.

Clientes

No menu Clientes, é possível efetuar configurações básicas para o trabalho com o cliente e grupos a serem administrados.

Novo grupo

Através deste comando, você pode criar um ***Grupo***. Em princípio, esta é uma pasta na camada de rede, onde você agrupa diversos clientes e pode trabalhá-los juntos. Com a ativação desse comando, aparece, abaixo da pasta que você marcou na área de seleção de clientes, um novo ícone de pasta no qual você pode atribuir diretamente um novo nome para esse grupo.

> **?** Para atribuir facilmente clientes individuais a esse grupo, você pode movê-los simplesmente para os respetivos registros de grupo. Através disso, esses clientes tornam-se subelementos dos respetivos grupos.

Editar grupos

Através desta opção, você abre uma caixa de diálogo na qual, através do botão **Adicionar** e **Remover**, pode agrupar clientes. Se não tiver selecionado nenhum grupo na área de seleção de clientes, essa função não poderá ser selecionada.

Excluir

Você pode remover um computador da lista de clientes a serem monitorados (***desativar***), marcando-o e selecionando o comando **Excluir** no menu Clientes. Observe que a desativação de um computador não faz com que o software cliente seja desinstalado.

Só excluir grupos quando o grupo estiver vazio. Ou seja, você deve desativar os clientes lá contidos ou mover para outros grupos. Clientes excluídos podem ser tornados novamente visíveis através da função **Exibir clientes desativados**.

Configurações padrão

Para a proteção de toda a rede ou de grupos selecionados, é possível criar configurações padrão e, com isso, criar predefinições padrão para a proteção antivírus rapidamente. Assim, você pode mover novos clientes em um grupo e, automaticamente, aplicar as configurações do grupo para esses clientes.

? As configurações padrão estão disponíveis na área de seleção de clientes, somente quando eles tiverem sido marcados ou o registro ***Toda a rede*** tiver sido selecionado. Novos clientes que forem integrados ao grupo assumem as configurações padrão e podem ser especificados posteriormente, se necessário.

? O significado que cada área de configuração individual e funções têm nas configurações padrão podem ser obtidos no capítulo **Configurações**

Excluir configurações padrão

As configurações padrão de um grupo podem ser excluídas através desta função. Dessa forma, as configurações padrão para toda a rede serão aplicadas aos respetivos grupos.

Atualizar exibição

Para acompanhar as alterações na rede que ocorrem periodicamente, utilizando o Administrator, é possível utilizar a função **Atualizar**.

Exibir clientes desativados

Os clientes que você não ***ativou*** ou que, através da função **Excluir**, removeu da lista de clientes ativos podem ser novamente exibidos através desta função. ***Os clientes desativados*** serão exibidos como ícones transparentes.

Ao contrário desses, os ***clientes ativos*** são definidos por meio de ícones coloridos.

Ativar cliente

Quando você seleciona um *G Data Client* desativado (exibido através de um ícone transparente) e pressiona **Ativar clientes** , esse será ativado.

Isto significa que ele estará disponível para observação. Nenhum controle de vírus estará vinculado a isso. Para isso, é preciso criar dados na área de tarefa **Sentinela** ou **Tarefas** ou atribuir o cliente a um grupo para o qual esses dados já são existentes. Assim que o *G Data Client* for instalado no computador cliente *observado* , a proteção de vírus estará disponível.

Ativar cliente (Diálogo)

Através desta função, é possível também ***Ativar clientes***, sem selecioná-los na área de opção de clientes. Ao pressionar essa função, aparece um campo de diálogo no qual basta inserir o nome do cliente que deverá ser ativado.

Procurar computador

Através dessa função, é possível solicitar a procura de computadores dentro de uma área definida de ***Endereços IP*** de sua rede. Basta informar o **Endereço IP inicial** e o **Endereço IP final**. O *G Data Software* procura agora automaticamente, em suas ***IDs de Host*** , por computadores vinculados. Você tem, então, a possibilidade de ativar os computadores encontrados. Através disso, é disponibilizada a possibilidade de ativá-los através de seus nomes de computador ou de comunicar-se diretamente com eles através do endereço IP. O respetivo cliente aparece com seu endereço IP na área de seleção de cliente.

Criar pacote de instalação do G Data Client

Através desta função, é possível criar um pacote de instalação para o *G Data Client*. O pacote é um arquivo executável único ***(AvkClientSetupPck.exe)*** com o qual um novo cliente, sem outras interações do usuário, pode ser instalado no computador a ser protegido. O pacote de instalação é especialmente adequado, por exemplo, para distribuir o cliente, através de script de login a todos os computadores de um domínio.

? O pacote contém sempre a versão atual do cliente no servidor. Na instalação do software cliente, você será perguntado se o ***G Data Firewall*** deverá também ser instalado em conjunto no computador cliente. Outras informações sobre o **Firewall** podem ser obtidas no capítulo de mesmo nome desta documentação.

Exibir

Através deste menu, é possível selecionar diferentes áreas de opção do software. As áreas exibidas são selecionadas por uma marcação. Através do item de menu **Atualizar**, é possível atualizar, a qualquer momento, a interface do programa, para p.ex., considerar também as alterações atuais na exibição. Informações sobre as áreas podem ser encontradas nos respetivos capítulos da ***Área de tarefas***.

Configurações

No menu Configurações, você tem acesso às configurações básicas do programa.

Atualização na Internet

Aqui você executa, na Internet, as atualizações dos bancos de dados de vírus e arquivos de programa do *G Data Software*. Primeiro, na guia **Dados de acesso e configurações** , insira os dados de acesso obtidos no ***Registro on-line***. Na atualização na Internet, os arquivos atuais do *G Data UpdateServer* são carregados e salvos no ManagementServer. A distribuição de novos arquivos aos clientes é controlada na área de tarefas **Clientes**. Com a atualização na Internet, você garante ter sempre os bancos de dados de assinaturas mais atuais e de dispor sobre os arquivos de programas mais recentes.

Banco de dados de vírus

Todos os clientes têm uma cópia do banco de dados de vírus, para que a proteção antivírus seja garantida também, quando estiverem offline (ou seja, nenhuma conexão ao ManagementServer). Isso é importante p.ex., para ***Notebooks***, que só estão conectados à rede de sua empresa em intervalos irregulares. A ***atualização*** dos arquivos nos clientes é feita em duas etapas que, naturalmente, podem ser ambas automatizadas. Na primeira etapa, são copiados os arquivos atuais do *G Data UpdateServer* em uma pasta no ManagementServer. Na segunda etapa os novos arquivos são distribuídos aos clientes (veja a Área de tarefas "Clientes").

- **Atualizar status**: Através desse botão, é possível atualizar também a exibição de status das assinaturas de vírus no cliente, caso as alterações ainda não tenham sido aplicadas à exibição.
- **Iniciar atualização agora**: Através do botão **Iniciar atualização agora**, você pode executar diretamente uma atualização do banco de dados de vírus.
- **Atualizações automáticas**: Como as verificações de vírus, as atualizações na Internet podem ser executadas automaticamente. Ative, para isso, a marcação em **Executar atualização periodicamente** que determina quando e o ciclo no qual a atualização deverá ser feita.

? Para que a atualização possa ocorrer automaticamente, o ManagementServer deverá naturalmente estar conectado à Internet ou o *G Data Software* deverá ser possibilitado a fazer uma discagem automática. Para isso, em **Dados de acesso e configurações** insira ***Conta de usuário*** e ***Configurações de proxy***.

Arquivos de programa

Quando o ***software Cliente*** for atualizado pela ***G Data***, a atualização pode ser feita automaticamente pelo ManagementServer. A ***atualização*** dos arquivos nos clientes é feita em duas etapas que, naturalmente, podem ser ambas automatizadas. Na primeira etapa, são copiados os arquivos atuais do *G Data UpdateServer* em uma pasta no ManagementServer. Na segunda etapa, os novos arquivos são distribuídos aos clientes e, com isso, o cliente é atualizado (veja a ***Área de tarefa Clientes***).

- **Atualizar**: Através do botão**Atualizar**, é possível atualizar também a exibição de status da versão de software para o cliente, caso as alterações ainda não tenham sido aplicadas à exibição.
- **Executar atualizações agora**: Através do botão **Executar atualizações agora**, você pode executar a atualização do software cliente.
- **Atualizações automáticas**: Como as verificações de vírus, as atualizações na Internet do software cliente podem ser executadas automaticamente. Ative, para isso, a marcação em **Executar atualização periodicamente** que determina quando e o ciclo no qual a atualização deverá ser feita.

? Para que a atualização possa ocorrer automaticamente, o ManagementServer deverá naturalmente estar conectado à Internet ou o *G Data Software* deverá ser possibilitado a fazer uma discagem automática. Para isso, em **Dados de acesso e configurações** insira ***Conta de usuário*** e ***Configurações de proxy***.

? ***Atenção***: Para atualizar os arquivos de programa do ManagementServer, abra no grupo de programas ***G Data ManagementServer***, no menu Iniciar, o registro ***Atualização na Internet***. O ManagementServer só pode ser atualizado através desse registro. Ao contrário do *software G Data Client*, que também pode ser atualizado através do Administrator.

Dados de acesso e configurações

Com o ***Registro on-line*** você obtém da ***G Data*** diretamente online, os dados de acesso para a atualização de seus bancos de dados de vírus e arquivos de programa. Em **Nome de usuário** e **Senha** insira os dados necessários. Através do botão **Verificação da versão** você pode, na próxima atualização do banco de dados de vírus definir se utilizará os arquivos de programa mais recentes. Por via de regra, a verificação da versão deverá sempre estar ativada, porque ela evita atualizações desnecessárias. Se no entanto ocorrerem problemas ao trabalhar com bancos de dados de vírus, desative o campo **Verificação da versão**. Dessa forma, na próxima atualização na Internet, uma versão atual do banco de dados de vírus será sobregravada no seu servidor. Com o botão **Conta do usuário e configurações de proxy**, você abre uma janela na qual poderá inserir os dados de acesso básicos para a Internet e a rede.

> ? ***Atenção***: Aqui você só deve fazer inserções quando ocorrerem problemas com as configurações padrão do *G Data Software* (p. ex., devido a utilização de um ***Servidor proxy***) e uma atualização na Internet não puder ser realizada.

Configurações da Internet

Para a sua conta do usuário, você precisa das informações: **Nome de usuário**, **Senha** e **Domínios**. Para o login no ***Servidor proxy***, é necessária, adicionalmente, a porta (usualmente: 80) e, caso diferente da conta do usuário, as informações sobre nome de usuário e senha para o servidor proxy.

> ? **Conta do usuário** é uma conta para o computador, no qual encontra-se o ManagementServer.

> ? O *G Data Software* pode ***utilizar os dados de conexão do Internet Explorer*** (a partir da versão 4). Configure primeiro o ***Internet Explorer*** e verifique se a página de teste de nosso servidor de atualização está acessível: ***http://ieupdate.gdata.de/test.htm***. Em seguida, você deve ativar a opção **Utilizar servidor proxy**. Em **Conta do usuário** , insira a conta configurada para o Internet Explorer (como a conta com a qual você fez o login em seu computador).

Mensagens de alarme

Em novas deteções de vírus, o ManagementServer pode, automaticamente, enviar mensagens de alarme por ***e-Mail***. As configurações necessárias para isso são realizadas nessa área.

Configurações de e-mail

Informe o nome do servidor de e-mail de sua rede, o **Servidor de SMTP** e a **Porta** (normalmente 25). Além disso, é necessário um endereço de remetente (válido) para que os e-mail possam ser enviados.

> **?** Esse endereço de e-mail também será usado para as respostas do ***Serviço antivírus emergencial*** .

Notificação por e-mail

Ative a notificação por e-mail colocando a marcação em **Enviar mensagens de alarme por e-mail** e, em **Destinatário**, o endereço de e-mail do destinatário das notificações. De qualquer modo, em **Limite**, você deve definir uma quantidade limite para que a caixa postal não fique lotada devido a graves infecções.

Notificação por telefone

Também é possível ser informado automaticamente por telefone pelo *G Data Software* sobre uma infecção de vírus. Em **Status**,esse serviço pode ser ativado ou desativado. Em **Anúncio** insira o texto que deverá ser lido no caso de um aviso de vírus e, em **Número de telefone**, o número de telefone onde estará acessível. Em **Janela de tempo** é possível, além disso, definir que o *G Data Software* só avise durante determinados horários. Para efetuar as configurações básicas para a notificação por telefone, abra, no grupo de programas "*G Data ManagementServer*" no menu Iniciar, o registro **Notificação por telefone (configurações)**. Aqui será possível fazer mais predefinições para o processo de discagem.

> **?** Observe que um prefixo local (normalmente o ***0***) deverá ser utilizado quando a chamada telefônica for encaminhada através de uma central telefônica para fora.

Reversão da atualização do mecanismo A / B

No caso de alarmes errados ou problemas semelhantes em raros casos, pode ser útil bloquear a ***Atualização de assinaturas de vírus*** e utilizar, ao invés dessas, uma das atualizações de assinaturas anteriores. O ManagementServer salva as últimas atualizações de cada mecanismo antivírus. Assim, se acontecerem problemas com a atualização do Mecanismo A ou B, o administrador pode bloquear a atualização por um determinado período e ao invés dessa, distribuir automaticamente a atualização de assinatura anterior, aos clientes e servidores da subrede.

> **?** Para clientes não conectados ao ManagementServer (como Notebooks em viagens de negócios) não será possível executar ***Reversões***. Um bloqueio transmitido pelo servidor ao cliente não poderá ser desfeito no mesmo.

> **?** A quantidade de reversões a serem salvas, pode ser configurada na área **Configurações do servidor** .

Configurações do servidor

Aqui é possível efetuar configurações básicas para as sincronizações e procedimentos de exclusão automáticos.

Configurações

Na área Configurações, você encontra as seguintes opções:

- **Reversões**: Informe aqui quantas atualizações de assinatura de vírus você deseja manter como reserva para as ***Reversões***. Como valor padrão, são válidas aqui as últimas dez atualizações de assinatura do respetivo mecanismo.

- **Limpar automaticamente**: Aqui é possível definir que ***registros de protocolo***, ***registros de verificação*** e ***Relatórios*** serão excluídos, automaticamente, após um determinado período.

Sincronização

Na área Sincronização, você pode definir temporalmente a comunicação entre clientes, servidores de subrede e servidores:

- **Clientes**: Insira aqui o intervalo de tempo no qual os clientes serão sincronizados ao servidor. Ao colocar a marcação em **Notificar os clientes quando houverem alterações de opções do servidor**, o usuário recebe um aviso, no computador cliente, informando que as alterações foram concluídas.

- **Servidor de subrede**: Através desta área, você pode definir intervalos para comunicação entre servidor e servidor de subrede. Ao colocar a marcação em **Transmitir imediatamente os novos relatórios para o servidor principal**, os relatórios serão transmitidos imediatamente ao servidor principal, independente das configurações efetuadas aqui.

Ajuda

Aqui você obtém informações sobre o programa e tem, além disso, a possibilidade de recorrer à ajuda online do *G Data Software*.

Barra de ferramentas

Na barra de ferramentas, encontram-se os principais comandos da ***Barra de menu*** como ícones clicáveis.

Novo grupo: os computadores ativados podem ser reunidos em ***grupos***. Com isso, é fácil definir diferentes zonas de segurança, porque todas as configurações, tanto para clientes individuais como também para grupos completos, podem ser executadas. Para criar um novo grupo, selecione primeiro o grupo superior e clique, em seguida, no ícone ilustrado.

Excluir: você pode remover um computador da lista ***(desativar)***, marcando-o e clicando no botão **Excluir**. Observe que a desativação de um computador não faz com que o software cliente seja desinstalado.

Atualizar exibição: através de **Atualizar** ou da tecla ***F5***, é possível atualizar, a qualquer momento, a interface do Administrator, para p.ex., considerar também as alterações atuais na exibição.

Exibir clientes desativados: selecione esse botão para também exibir os computadores não ativados. Você reconhece os computadores desativados pelos ícones cinzas transparentes. Computadores sem liberação de arquivos ou de impressoras não são exibidos normalmente.

Ativar cliente: para ativar um computador, selecione-o na lista e escolha o botão ilustrado. Você também pode ativar computadores que não estão relacionados na lista. Para isso, selecione, no menu Clientes, o comando **Ativar cliente (Diálogo)** e dê o nome do computador.

Exibir registro: através do arquivo de registro, você tem uma rápida visão global sobre as últimas ações do *G Data Software*. Aqui são exibidas todas as informações relevantes.

Atualização na Internet: através da área ***Atualização na Internet***, você executa as atualizações dos bancos de dados de vírus e dos arquivos de programa do cliente na Internet.

Mensagens de alarme: em novas deteções de vírus, o ManagementServer pode, automaticamente, enviar mensagens de alarme por e-Mail. As configurações necessárias para isso são efetuadas na área **Mensagens de alarme** no menu **Configurações**.

Ajuda: através desse botão, você tem a possibilidade de acessar ajuda online da *G Data* .

Área de Seleção de clientes, encontrada à esquerda,

Aqui você encontra todos os clientes e servidor, assim como grupos definidos em sua rede, relacionados e subdivididos hierarquicamente. Como no Windows Explorer, aparecem grupos nos quais existem subdivisões com um pequeno sinal de mais. Ao clicar neles, aparece a estrutura do diretório neste ponto e possibilita a visualização da estrutura por trás. Um clique no sinal de menos fecha novamente essa subdivisão. Estão disponíveis os seguintes ícones na seleção de diretórios:

Ícone da rede

Grupos

Servidor (ativado)

 Servidor (desativado)

 Cliente (ativado)

 Cliente (desativado)

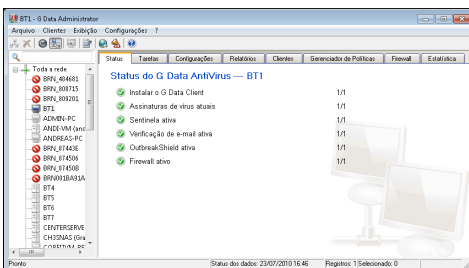
 Dispositivos não selecionáveis: Aqui caem, por exemplo, a impressora da rede

Área de tarefas

Nas diversas áreas de tarefas, que podem ser selecionadas através das respectivas guias, você tem a possibilidade de administrar confortavelmente a proteção de seus clientes. As configurações efetuadas estão sempre relacionadas aos clientes ou grupos que foram selecionados ou marcados na ***área de Seleção de Clientes***. Os diferentes campos de tópicos são descritos de forma detalhada nos próximos parágrafos.

- **Status**
- **Tarefas**
- **Configurações**
- **Relatórios**
- **Clientes**
- **Gerenciador de Políticas**
- **Firewall**
- **Estatística**

Status

Na área Status do *G Data Software* você obtém informações básicas sobre a situação atual do seu sistema. Essas podem ser encontradas à direita do respectivo registro como informações em texto, número ou data.

Enquanto o seu sistema estiver idealmente configurado para a proteção contra vírus, você encontrará, à esquerda dos registros aqui relacionados, um sinal verde.

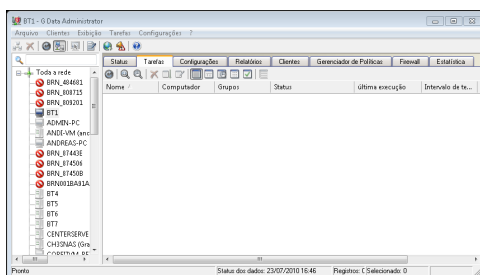
Se um componente não estiver configurado adequadamente (p. ex., a sentinela desativada ou assinaturas de vírus desatualizadas), um sinal de aviso indicará isso.

? Quando a interface do programa *G Data* abre, a maioria dos ícones encontra-se no modo de atenção. Isso não significa que seu computador não está protegido, nesse momento, pelo *G Data Software*. Pelo contrário, aqui trata-se de uma verificação interna do status de proteção antivírus, indicando que no momento, uma verificação automática das funções está ocorrendo.

Através de um clique duplo no respetivo registro, é possível executar ações diretamente ou alterar para a respetiva área da tarefa. Assim que tiver otimizado as configurações de um componente com o ícone de atenção, ele torna-se novamente para o sinal verde na área de status.

Tarefas

Nesta área de tarefas, é possível definir tarefas para as verificações de vírus nos *G Data Clients*. Existem dois tipos diferentes de tarefas: ***Tarefas de verificação únicas*** e ***tarefas de verificação periódicas***. As tarefas únicas são executadas diretamente após sua criação, para as periódicas é definida uma ***Programação*** de acordo com a qual a tarefa deverá ser executada.

> **?** ***Tarefas de verificação*** ou ***tarefas*** são as respectivas tarefas criadas na área de tarefas de mesmo nome para controle, remoção ou profilaxia de vírus.

Na área **Tarefas,** aparecem todas as tarefas sob os nomes designados por você e as mesmas podem ser organizadas através de um clique na respectiva designação da coluna, pelos diferentes critérios a seguir. A coluna, de acordo com a qual a classificação atual é feita, é marcada através de uma pequena seta:

- **Nome**: O nome definido por você para uma tarefa de verificação. Aqui é possível inserir nomes longos, como desejado, e assim descrever a sua tarefa de verificação de forma extra para manter a visão geral sobre as diferentes tarefas.
- **Computador**: Aqui você encontra os nomes dos respetivos clientes. Você só pode definir tarefas de verificação para clientes ativos.
- **Grupos**: Você pode reunir clientes individuais em grupos que utilizarão, então, a mesma tarefa de verificação. Quando você atribui uma tarefa de verificação a um grupo, aparece, na lista de visão geral, não os computadores individuais, mas sim, o nome dos grupos.
- **Status**: Aqui você obtém a exibição do status ou o resultado de uma tarefa de verificação em texto claro. Desta forma, você descobre se a tarefa foi executada ou concluída e será informado se vírus foram ou não detetados.
- **Última execução**: Através dessa coluna, você obtém informações sobre quando a respetiva tarefa de verificação foi executada pela última vez.

- **Intervalo de tempo**: De acordo com a ***Programação*** que você pode definir para cada tarefa de verificação, é exibido aqui o ciclo no qual a tarefa será repetida.
- **Escopo da análise**: Aqui você descobre quais ***mídias de dados*** (p.ex., discos rígidos locais) a análise abrange.

? Na barra de menu, está disponível um registro adicional para a área **Tarefas** com as seguintes funções:

- **Exibição**: Selecione aqui se todas as ***tarefas de verificação***, somente tarefas de verificação únicas, periódicas ou em aberto, ou apenas as tarefas de verificação concluídas devem ser exibidas. Para as tarefas de verificação que foram definidas para um ***Grupo*** de clientes, é possível definir se as informações detalhadas deverão ser exibidas para todos os clientes ou apenas resumos para grupos. Coloque, para isso, uma marcação em **Exibir as tarefas de grupo detalhadamente**.
- **Executar novamente (imediatamente)**: Aqui você pode executar diretamente as tarefas de verificação selecionadas, independentemente dos dados temporais configurados.
- **Cancelar**: Através desta função é possível cancelar uma tarefa de verificação em execução.
- **Excluir**: As tarefas de verificação selecionadas podem ser excluídas com essa função.
- **Novo**: Selecione aqui se deseja criar uma ***tarefa de verificação única*** (uma única verificação) ou uma ***tarefa de verificação regular*** (verificação periódica).

Você pode definir, como desejado, diferentes tarefas de verificação. Em geral, devido ao desempenho, é sensato não sobrepor temporalmente as tarefas de verificação.

Atualizar

Essa função atualiza a visualização e carrega a lista de tarefas atual do ManagementServer.

Nova tarefa de verificação (única)

Com esta função, você cria uma nova tarefa para verificação única. Um diálogo é aberto para as configurações de tarefas e parâmetros de verificação. Aqui é possível inserir as predefinições desejadas. Alterne entre as áreas de configuração, simplesmente selecionando a respetiva guia. Essas guias serão explicadas detalhadamente no capítulo **Nova tarefa de verificação (periódica)**.

? Através da função **Nova tarefa de verificação (periódica)** você tem a possibilidade de definir tarefas de verificação controladas por tempo, as quais o seu sistema verificará automaticamente em intervalos regulares.

? Dê um clique duplo para alterar o parâmetro de uma tarefa existente no registro ou selecione no menu contextual (clicando com o botão direito do mouse) o comando ***Propriedades***. Agora será possível alterar, como desejado, as configurações das tarefas de verificação.

Nova tarefa de verificação (periódica)

Com esta função, você cria uma nova tarefa para verificação periódica. Um diálogo é aberto para as configurações de tarefas e parâmetros de verificação. Aqui é possível inserir as predefinições desejadas. Alterne entre as áreas de configuração, simplesmente selecionando a respetiva guia:

? Dê um clique duplo para alterar o parâmetro de uma tarefa existente no registro ou selecione, no menu contextual (clicando com o botão direito do mouse), o comando ***Propriedades***. Agora será possível alterar, como desejado, as configurações das tarefas de verificação.

Tarefa

Defina, nos parâmetros da tarefa, o nome que a tarefa de verificação deverá ter. Aqui você pode usar nomes significativos como ***Verificação de pastas*** ou ***Verificação mensal*** para caracterizar claramente a tarefa desejada e reencontrá-la na visão geral em tabela. Além disso, é possível informar se o usuário pode cancelar a tarefa através do menu contextual do cliente. Se sua rede tiver de ser permanentemente monitorada com a sentinela, é justificável possibilitar ao usuário cancelar a tarefa de verificação, porque a mesma poderá influenciar facilmente seu ritmo de trabalho. Se, no entanto, você não desejar usar a sentinela, os procedimentos de verificação periódicos, especialmente, não podem ser negligenciados e não devem ser desativáveis. Através da opção **Transmitir progresso da verificação regularmente para o servidor** , você pode solicitar a exibição do status de um procedimento de verificação em um cliente, por meio de dados percentuais. Com a função **Desativar o computador após a verificação de vírus, se nenhum usuário estiver conectado** , você tem mais uma opção que ajuda a reduzir o trabalho administrativo.

Período/Programação

Nessa guia, é possível definir quando e em que ritmo a atualização automática deverá ocorrer. Em **Executar** insira uma predefinição que você pode especificar em **Período** e **Dias da semana**. Se você selecionar **Na inicialização do sistema**, as predefinições da programação continuarão e o *G Data Software* executará a atualização sempre que o seu computador for reinicializado.

> **?** Em **Diariamente**, é possível definir com o auxílio dos dados em **Dias da semana** que, p.ex., o seu computador só executará a atualização em dias úteis ou mesmo a cada dois dias ou, nos fins de semana onde ele não é utilizado para trabalhar.

Verificador

No menu Verificador, você pode definir como o *G Data Software* deverá proceder na verificação de vírus. Como uma verificação de vírus com base em uma programação ou um início de análise manual deve ocorrer em momentos nos quais o computador não está totalmente sobrecarregado com outras tarefas, em geral, aqui podem ser utilizados mais recursos de sistema para a análise de vírus do que para a ***Sentinela de vírus***.

- **Utilizar mecanismos:**: O *G Data Software* trabalha com dois mecanismos antivírus; duas unidades operacionais de análise independentes uma da outra. Em princípio, a utilização dos dois mecanismos é a garantia para os resultados ideais da profilaxia de vírus. A utilização de um único mecanismo, ao contrário, oferece vantagens de desempenho; ou seja, ao utilizar apenas um mecanismo, o processo da análise pode ocorrer mais rapidamente. Recomendamos a configuração **Ambos os mecanismos - desempenho otimizado**. Através dessa, os verificadores de vírus estão tão interligados entre si que permitem o reconhecimento ideal no tempo de verificação mínimo.

- **No caso de uma infecção**: Aqui você pode definir o que deve ocorrer na deteção de um arquivo infectado. Dependendo do fim para o qual o respetivo cliente é utilizado, diferentes configurações são recomendáveis. A configuração **Mover arquivos para a quarentena** trata-se de um diretório especial que o ManagementServer cria, no qual os arquivos infectados são codificados e não podem mais criar funções danosas contínuas. Os arquivos na ***Quarentena***podem ser desinfectados pelo Adminisrator, excluídos, movidos para o local original ou, eventualmente, enviados para o ***Serviço antivírus emergencial*** da ***G Data***.

- **Pastas infectadas**: Defina aqui se o tratamento de deteções de vírus para ***Pastas compactadas*** deverá ser diferente. Deve-se considerar que um vírus fora de uma pasta compactada só causa danos quando a mesma for descompactada.

- **Tipos de arquivos**: Aqui é possível definir em quais tipos de arquivos o *G Data* deverá examinar quanto à existência de vírus. Por via de regra, não é necessário verificar arquivos que não contenham nenhum código de programa executável; até porque, uma verificação de todos os arquivos de um computador pode levar um determinado tempo.

- **Verificador prioritário**: Através dos níveis ***alta***, ***média*** e ***baixa*** é possível determinar se uma verificação de vírus, através do *G Data* no seu sistema, deverá ter alta prioridade (nesse caso, a análise é feita de forma relativamente rápida, outros aplicativos ficarão possivelmente mais lentos durante a análise) ou baixa prioridade (a análise ocorre relativamente lenta, mas os outros aplicativos funcionam quase sem interrupções nesse tempo). Dependendo da hora em que a análise de vírus é executada, diferentes configurações são úteis.

- **Configurações**: Defina, aqui, as análises de vírus adicionais que o *G Data Software* deverá executar. As opções aqui selecionadas são totalmente recomendáveis; dependendo do tipo de utilização, a vantagem da economia de tempo através da não verificação pode comprometer um pouco a segurança. Para isso, as seguintes possibilidades estão disponíveis:

    Heurística: Na heurística, são apurados os vírus, não apenas com o auxílio de bancos de dados atualizados continuamente, mas também com a ajuda de características específicas, típicas de vírus. A heurística pode, em raros casos, criar um alarme falso.

    Pastas compactadas: A verificação de dados compactados em pastas é demorada e pode ser ignorada quando a ***Sentinela G Data*** estiver ativa no sistema. Ela reconhece na descompactação um vírus oculto até o momento e, impede automaticamente a sua propagação. Mesmo assim, no controle constante fora do tempo de operação real do computador, deverá ocorrer também um controle das pastas compactadas.

    Pastas de e-mail: A verificação de dados compactados em pastas de e-mail é demorada e pode ser ignorada quando a ***Sentinela G Data*** estiver ativa no sistema. Ela reconhece na descompactação um vírus oculto até o momento e, impede automaticamente a sua propagação. Mesmo assim, no controle constante fora do tempo de operação real do computador, deverá ocorrer também um controle das pastas compactadas.

    Áreas do sistema: A área do sistema de seus computadores ***(setores de boot, Master Boot Records e etc.)*** que oferecem uma base fundamental para o sistema operacional, não devem ser, em geral, excluídas do controle de vírus.

Verificar Discador/Spyware/Adware/Riskware: Com o *G Data Software*, o seu sistema pode ser verificado também quanto a ***Discadores*** e outros softwares maliciosos (***Spyware***, ***Adware***, ***Riskware***). Aqui se trata de programas que estabelecem caras e indesejadas conexões à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, já que, p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.

Verificar a existência de Rootkits: Os ***Rootkits*** tentam escapar dos métodos comuns de detecção de vírus. Com essa função é possível procurar por Rootkits de forma objetiva, sem ter que executar uma verificação completa dos discos rígidos e dados armazenados.

Utilizar todos os processadores disponíveis: Com essa opção, você pode distribuir o controle de vírus em sistemas com diversos ***Processadores*** (p.ex., DualCore) e, dessa forma, executar uma verificação de vírus de forma claramente mais rápida. A desvantagem dessa opção é a velocidade de trabalho do sistema, que será freiada para outros aplicativos. Portanto, essa opção só deverá ser utilizada quando a sua tarefa de verificação for realizada em momentos em que o sistema não é utilizado regularmente (como noites)

Escopo da análise

Através da guia **Escopo da análise** é possível limitar no cliente o controle de vírus também em determinados diretórios. Dessa forma, é possível poupar pastas compactadas raramente utilizadas ou integrá-las em um esquema de verificação especial. A seleção de diretórios baseia-se no computador selecionado no momento e não no cliente selecionado.

? ***Particularidade em tarefas de verificação em um servidor de arquivos Linux***: Na seleção de diretório, a unidade raiz (/) e todas as liberações são devolvidas. Assim, tarefas de verificação podem ser executadas objetivamente em liberações selecionadas ou diretórios escolhidos de acordo com o desejado em servidores de arquivo.

Excluir tarefas de verificação

A função **Excluir tarefas de verificação**, exclui todas as tarefas selecionadas.

Executar novamente tarefas de verificação (imediatamente)

Selecione essa função para executar novamente tarefas de verificação únicas que já foram executadas ou que foram canceladas. No caso de tarefas de verificação periódicas, essa função faz com que a verificação seja executada imediatamente independente da programação.

Registros

Abra, com esta função, os registros para as tarefas dos respetivos clientes.

Opções de exibição

No caso de uma grande quantidade de diferentes relatórios, é útil solicitar a exibição de acordo com diferentes critérios e em uma listagem. As seguintes possibilidades estão disponíveis:

Exibir todas as tarefas

Exibir somente tarefas de verificação únicas

Exibir somente tarefas de verificação periódicas

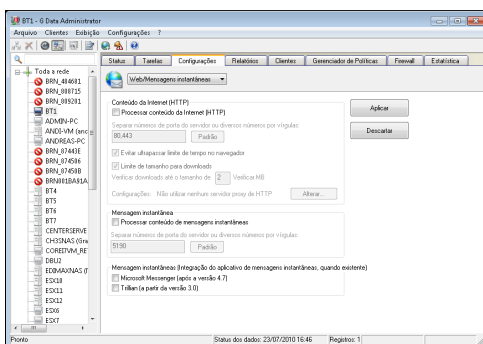
Exibir somente tarefas de verificação em aberto

Exibir somente tarefas de verificação concluídas

Exibir as tarefas de grupo detalhadamente: Exibe as tarefas de grupo de todos os registros correspondentes. A opção só está disponível quando um grupo estiver selecionado na lista de computadores.

Configurações

Nesta área de tarefas, é possível fazer configurações de opções pra todos os clientes, clientes individuais ou um grupo de clientes (p.ex., se as atualizações deverão ser feitas automaticamente, se atualizações próprias da Internet são permitidas através do cliente, se diretórios de exceções podem ser definidos lá individualmente e etc.).

Através da caixa de seleção localizada acima, é possível decidir que tipo de opções você deseja editar através dela. Para isso, na ***área de Seleção de clientes,*** selecione o cliente desejado ou o grupo de clientes que deseja configurar, pressione os dados desejados e conclua o procedimento clicando no botão **Aplicar**.

Geral

Aqui você tem as seguintes possibilidades de configuração:

G Data Client

As seguintes funções estão disponíveis:

- **Comentário**: Insira aqui um nome significativo para o respetivo cliente.

- **Ícone na barra de inicialização**: Para servidor de terminal e Windows com rápida alternância de usuários, pode-se escolher em que sessões um ícone do cliente deverá ser exibido na barra de tarefas: ***nunca***, ***somente na primeira sessão*** ou ***sempre***. Nos clientes *normais*, a opção de exibição do ícone do cliente pode ser impedida por opção. Para que o usuário tenha acesso a funções avançadas do cliente, o ícone precisa ser exibido, porque dessa forma, pode-se acessar por clique do mouse, o***Menu contextual*** correspondente.

- **Conta do usuário**: O software cliente é normalmente executado no contexto do sistema. Você pode inserir aqui uma nova conta para possibilitar a verificação de diretórios da rede. A conta deverá, para isso, ter direitos de administrador no cliente.

Atualizações

As seguintes funções estão disponíveis:

- **Atualizar assinaturas de vírus automaticamente**: Ativa a atualização automática do banco de dados de vírus. Os clientes verificam periodicamente se existe uma nova versão do ManagementServer e executam automaticamente a atualização.

- **Atualizar arquivos de programa automaticamente**: Atualiza os arquivos de programa no cliente com os arquivos do ManagementServer. Após a atualização dos arquivos de programa, pode ser que o cliente tenha que ser reiniciado. Dependendo da configuração em **Reiniciar após a atualização** o usuário terá a possibilidade de, no cliente, ratardar a atualização dos dados para um período posterior.

- **Reiniciar após a atualização**: Aqui é possível definir se o cliente, em uma atualização dos arquivos do programa, será automaticamente reinicializado (**Reiniciar sem perguntar**), ou se será oferecida a possibilidade ao usuário de executar a reinicialização imediatamente ou depois **(Abrir janela de observações no cliente)** ou se a atualização dos arquivos de programa só ocorrerá quando o cliente for reiniciado por si mesmo (**Gerar relatório**).

Recursos do cliente

Com as funções a seguir, você define aparência, comportamento e abrangência da função do respetivo cliente. Dependendo da predefinição, o usuário tem, dessa forma, direitos abrangentes ou restritos, ou apenas direitos fortemente restritos em relação à profilaxia e ao combate a vírus:

- **O usuário pode executar, ele mesmo, as atualizações de vírus**: No caso de suspeita grave, o usuário pode, como em uma solução de vírus instalada localmente, realizar, ele mesmo e de forma independente do ManagementServer, uma ***Verificação de vírus***. Os resultados dessa verificação de vírus serão transmitidos para o ManagementServer no próximo contato.

- **O usuário pode, ele mesmo, carregar as atualizações de assinaturas**: Quando você ativa essa função, as assinaturas de vírus do respetivo cliente podem ser carregadas, mesmo sem conexão ao servidor da empresa, diretamente da Internet. Isso aumenta significativamente a segurança, mesmo em notebooks utilizados em serviços externos.

- **O usuário pode alterar as opções de e-mail e de sentinela**: Na ativação dessa função, o usuário cliente tem a possibilidade, objetivamente, além das ***opções de sentinela,*** de influenciar a configuração sobre o tópico ***Segurança de e-Mail:*** para o seu cliente.

- **Exibir quarentena local**: Quando você permite a exibição da ***Quarentena*** local, o usuário pode desinfectar, excluir ou restaurar dados que foram movidos pela sentinela para a pasta de quarentena, devido à infecção de vírus ou suspeita. Observe que, em uma restauração, o vírus não terá sido removido. Portanto, essa opção só deve ser possibilitada a usuários avançados nos clientes.

- **Proteção por senha para alterações de opções**: Quando o usuário recebe o direito de alterar as opções de sentinela no cliente, existe, naturalmente, sempre a possibilidade de que outras pessoas, nesse computador, desativem indevidamente as funções de sentinela. Para evitar isso, é possível proteger as configurações das opções de sentinela no cliente, com uma senha. Atribua a senha, aqui, de forma individual para o respetivo cliente ou grupo e informe aos usuários autorizados do computador cliente.

- **Configurações da atualização**: Aqui é possível definir se a atualização, na Internet, das assinaturas de vírus deverão ser feitas de forma central através do servidor, individualmente para cada cliente ou combinado. Principalmente em locais de trabalho móveis que só eventualmente são conectados à rede da empresa, recomenda-se uma combinação das variantes. Através do botão **Configurações e programação** , é possível, além disso, definir, para o respetivo cliente, configurações relacionadas para as assinaturas de vírus.

Diretório de exceções para tarefas de verificação

Aqui é possível definir diretórios de exceção para os clientes, os quais não deverão ser verificados durante a execução de tarefas de verificação. As áreas de pastas compactadas e backup de um disco rígido ou partição podem, por exemplo, serem definidas como diretórios de exceção.

? Diretórios de exceções podem ser definidos para ***grupos*** inteiros. Caso o cliente em um grupo tenha definido diferentes diretórios de exceção, novos diretórios poderão ser adicionados ou os existentes poderão ser excluídos. Os diretórios definidos especialmente para clientes individuais permanecem preservados. O mesmo procedimento é utilizado também nas exceções da sentinela.

? ***Particularidade para um servidor de arquivos Linux***
Na seleção de diretórios de exceção, a unidade raiz (/) e todas as liberações são entregues de volta. Assim, é possível definir exceções para unidades, diretórios e máscaras de arquivos.

Sentinela

Aqui podem ser feitas as configurações de sentinela para os clientes selecionados na ***área de Seleção de clientes***. Selecione um grupo para alterar as configurações de sentinela de todos os clientes do grupo. Na área **Sentinela,** é possível fazer configurações individuais para cada cliente/grupo. As configurações alteradas só serão armazenadas e aplicadas pelo cliente após a pressão no botão **Aplicar**. Pressione o botão **Descartar** para carregar as configurações atuais do ManagementServer, sem aplicar as alterações.

? Ao editar as configurações da sentinela de um ***grupo,*** os parâmetros individuais podem receber um status indefinido. Os clientes do grupo, neste caso, têm diferentes configurações para o parâmetro. Parâmetros indefinidos não são armazenados durante a aplicação.

Primeiro, você não deve nunca desativar a sentinela sem uma razão plausível, porque ela contribui consideravelmente para a segurança de sua rede. Assim que tiver ativado a sentinela em um cliente, essa permanecerá sempre ativa em segundo plano.

? Na utilização de determinados programas ou componentes, podem ocorrer retardos significativos (p.ex., ***T-Online***, ***Microsoft Office*** com determinadas ***impressoras HP***). Para evitar isso, é possível definir os arquivos INI desses produtos como exceções. Isso reduz consideravelmente o processo de verificação, mas impõe um certo risco de segurança. Aqui é preciso ponderar.

Configurações

As seguintes informações estão disponíveis na área de configurações:

- **Status da sentinela**: Aqui é possível ativar ou desativar a sentinela. Em geral, a sentinela deverá permanecer ativa. Ela é a base para uma proteção antivírus permanente e sem falhas.

- **Utilizar mecanismos:**: O *G Data Software* trabalha com duas unidades de análise de vírus independentes uma da outra. Em princípio, a utilização de ambos os mecanismos é a garantia para os resultados ideais da profilaxia de vírus. A utilização de apenas um mecanismo traz, por outro lado, vantagens de desempenho.

- **No caso de uma infecção**: Aqui você pode definir o que deve ocorrer na deteção de um arquivo infectado. Dependendo do fim para o qual o respetivo cliente é utilizado, diferentes configurações são recomendáveis.

  Bloquear acesso ao arquivo: Em um arquivo infectado, não poderão ser executados acessos de leitura ou gravação.

  Desinfectar (se não for possível: Bloquear acesso): Aqui se tenta remover o vírus; se isso não for possível, o acesso ao arquivo é bloqueado.

Desinfectar (se não for possível: para quarentena): Aqui se tenta remover o vírus; se isso não for possível, o acesso ao arquivo é movido para a ***Quarentena*** .

Desinfectar (se não for possível: Excluir arquivo: Aqui se tenta remover o vírus; se isso não for possível, o acesso ao arquivo é excluído.

Mover arquivos para a quarentena: Aqui o arquivo infectado é movido para a quarentena Uma possível desinfecção do arquivo pode ser executada manualmente pelo administrador do sistema.

Excluir arquivo infectado: Como medida rigorosa, essa função ajuda a bloquear o vírus de forma eficaz. No entanto, podem ocorrer - dependendo do vírus - perdas significativas de dados.

- **Pastas infectadas**: Defina aqui se o tratamento de deteções de vírus para pastas deverá ser diferente. Deve-se considerar que um vírus fora de uma pasta compactada só causa danos quando a mesma for descompactada.

- **Tipos de arquivos**: Aqui é possível definir quais os tipos de arquivos que o *G Data Software* deverá examinar quanto à existência de vírus. Por via de regra, não é necessário verificar arquivos que não contenham nenhum código de programa executável; até porque, uma verificação de todos os arquivos de um computador pode levar um determinado tempo.

- **Verificar durante a gravação**: Normalmente um sistema sem vírus não cria naturalmente, ao gravar arquivos, nenhum arquivo infectado. No entanto, para excluir qualquer eventualidade, principalmente em sistemas nos quais nenhum ***BootScan*** foi executado, é possível definir aqui um procedimento de verificação ao gravar arquivos. A imensa vantagem está no fato de que, assim, os vírus, os quais são copiados de um outro cliente, possivelmente desprotegido, para um diretório liberado e protegido pela sentinela, podem também ser detetados, além de que arquivos carregados da Internet, já no processo de carregamento e não na execução, já serem reconhecidos como infectados por vírus.

- **Verificar acessos à rede**: Aqui é possível definir o procedimento da sentinela em relação aos acessos à rede. Quando você monitora toda a sua rede, em geral com o *G Data Software*, um monitoramento dos acessos à rede não é necessário.

- **Heurística**: Na análise heurística, os vírus são reconhecidos não apenas com o auxílio de bancos de dados atualizados continuamente, mas, também, com a ajuda de características específicas típicas de vírus. Esse método é mais uma vantagem de segurança; no entanto, em raros casos, pode levar também à criação de um ***alarme falso***.

- **Verificar pastas (compactadas)**: A verificação de dados compactados em pastas é bastante dispendiosa em tempo e pode geralmente ser ignorada quando a *Sentinela de vírus G Data* estiver ativada no sistema. Ela reconhece na descompactação um vírus oculto até o momento e, impede automaticamente a sua propagação. Para não sobrecarregar o desempenho através da verificação desnecessária de arquivos compactados utilizados raramente, é possível limitar o tamanho dos arquivos compactados que serão verificados, para um valor específico em kilobyte.

- **Verificar pastas de e-mail**: Essa opção deve, em geral, ser desativada, porque a verificação de pastas compactadas de e-mail normalmente demora muito e, no caso de um e-mail infectado, nenhum outro e-mail poderá mais ser lido. Como a sentinela bloqueia a execução de anexos de e-mail infectados, nenhuma brecha de segurança é criada através da desativação dessa opção. Na utilização do ***Outlook***, os e-mails de entrada e saída serão verificados adicionalmente através de um plugin integrado.

- **Verificar áreas do sistema na inicialização do sistema**: As áreas de sistema (p.ex., ***setores de boot***) do seu computador não devem ser ignoradas no controle de vírus. Aqui você pode definir se essas devem ser verificadas na inicialização do sistema ou na troca de mídia (novo CD-ROM ou similar). Normalmente, pelo menos uma dessas duas funções deve estar ativada.

- **Verificar áreas de sistema na troca de mídia**: As áreas de sistema (p. ex., ***setores de boot***) do seu computador não devem ser ignoradas no controle de vírus. Aqui você pode definir se essas devem ser verificadas na inicialização do sistema ou na ***troca de mídia*** (novo CD-ROM ou similar). Normalmente, pelo menos uma dessas duas funções deve estar ativada.

- **Verificar Discador/Spyware/Adware/Riskware**: Com o *G Data Software*, o seu sistema pode ser verificado também quanto a ***Discadores*** e outros softwares maliciosos (***Spyware***, ***Adware***, ***Riskware***). Aqui se trata de programas que estabelecem caras e indesejadas conexões à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, já que, p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.

Exceções

Aqui é possível limitar, no cliente, o controle de vírus também para determinados diretórios. Dessa forma, é possível poupar pastas compactadas raramente utilizadas ou integrá-las a um esquema de verificação especial. Além disso, determinados arquivos e tipos de arquivos podem ser excluídos da verificação de vírus. As seguintes excessões são possíveis:

- **Unidade**: Selecione aqui, com um clique no botão Diretório, uma unidade (***Partição***, ***disco rígido***) a qual você não deseja que a sentinela controle.
- **Diretório**: Selecione aqui, com um clique no botão Diretório, uma ***Ordner*** (eventualmente suas ***subpastas***), que não devem ser controladas pela sentinela.
- **Arquivo**: Aqui é possível inserir o nome do arquivo que deseja que o controle da sentinela ignore. Aqui é possível também trabalhar com espaços reservados (p.ex. o sinal de interrogação (?) para um caracter qualquer ou o asterisco (*) para uma sequência desejada de caracteres).

Esse processo pode ser repetido quantas vezes desejado e, na janela **Exceções da sentinela**, pode-se excluir ou modificar novamente as exceções existentes.

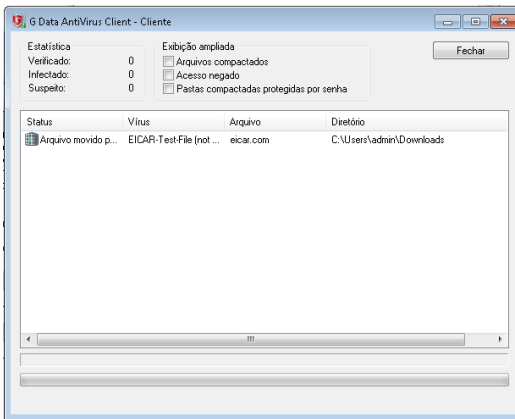
? A forma de funcionamento dos ***Espaços reservados*** é a seguinte:

- O ***ponto de interrogação*** (?) é substituto para caracteres individuais.
- * O ***asterisco*** (*) é substituto para seqüências de caracteres inteiras.

Para proteger todos os arquivos com a extensão de arquivo ***exe***, digite ****.exe***. Para proteger p.ex., formatos de planilhas diferentes

(p.ex.,***.xlr**, ***.xls**), basta digitar ***.xl?**. Para verificar, p.ex., tipos diferentes de arquivos com um nome de arquivo de início igual, digite, por exemplo, ***texto*.***.

Mensagens de aviso

Aqui é possível definir se o Usuário será notificado no computador cliente sobre um Vírus detectado. Quando a marcação estiver colocada aqui, aparece no usuário uma janela informativa a qual informará sobre o vírus detectado.

Status

Aqui será exibido se as alterações efetuadas na sentinela já foram aplicadas para o cliente ou grupos ou se o botão **Aplicar** ainda não foi pressionado.

E-Mail

Em cada *G Data Client,* é possível configurar uma proteção antivírus especial para e-mails. Aqui são verificados os protocolos ***POP3***, ***IMAP*** e ***SMTP*** para a camada ***TCP/IP***. Para o ***Microsoft Outlook,*** existe, além disso, um ***PlugIn*** especial para utilização. O plugin verifica automaticamente todos os e-mails de entrada quanto a existência de vírus e impede que e-mails infectados sejam enviados. Com o botão **Aplicar,** você estará aceitando as alterações executadas e, com **Cancelar,** você sai do diálogo sem aplicar as alterações executadas. Através do Administrator, é possível definir configurações individuais para cada cliente ou grupo de usuários para o trato de e-mails. Você tem, para isso, as seguintes opções:

E-mails de entrada

As seguintes funções estão disponíveis:

- **No caso de uma infecção**: Aqui você pode definir o que deve ocorrer na deteção de um arquivo infectado. Dependendo do fim para o qual o respetivo cliente é utilizado, diferentes configurações são recomendáveis.

- **Verificar a existência de vírus nos e-mails recebidos**: Com a ativação dessa opção, todos os e-mails que chegam ao cliente são verificados quanto à existência de vírus.

- **Verificar e-mails não lidos no início do programa (somente no Microsoft Outlook)**: Essa opção serve para controlar a infecção de vírus em e-mails que chegam ao cliente durante a sua conexão com a Internet. Portanto, assim que o ***Outlook*** é aberto, todos os e-mails não lidos na pasta caixa de entrada e suas sub-pastas serão controlados.

- **Anexar relatório aos e-mails recebidos e infectados**: Assim que um e-mail enviado ao cliente contém um vírus, você recebe no corpo desse e-mail, abaixo do texto original, o aviso ***ATENÇÃO! Este e-mail contém o seguinte vírus*** seguido pelo nome do vírus. Além disso, antes do assunto real, aparece a mensagem ***[VÍRUS]***. Se tiver ativado a opção **Excluir anexo/texto**, será informado, além disso, que a parte infectada do e-mail foi removida.

E-mails de sada

As seguintes funções estão disponíveis:

- **Verificar e-mails antes do envio**: Para que, da sua rede, vírus não sejam enviados inadvertidamente, o *G Data Software* oferece também a possibilidade de verificar a existência de vírus em e-mails antes do envio. Se realmente um vírus for enviado, aparece o aviso ***de que o e-mail [Linha de assunto] contém os seguintes vírus: [Virusname]***. O e-mail não pode ser enviado e o respetivo e-mail não será enviado.

- **Anexar relatório aos e-mails de saída**: Um relatório de verificação é anexado ao corpo de cada e-mail de saída abaixo do texto original do e-mail. Esse dirá que ***o G Data AntiVirus verificou a existência de vírus*** , enquanto a opção **Verificar e-mails antes do envio** estiver ativada. Além disso, a data da versão do *G Data AntiVirus* (**Informação sobre a versão**) pode ser informada.

Opções de varredura

As seguintes funções estão disponíveis:

- **Utilizar mecanismos:**: O *G Data Software* trabalha com dois mecanismos antivírus; duas unidades operacionais de análise independentes uma da outra. Em princípio, a utilização dos dois mecanismos é a garantia para os resultados ideais da profilaxia de vírus. A utilização de um único mecanismo, ao contrário, oferece vantagens de desempenho; ou seja, ao utilizar apenas um mecanismo, o processo da análise pode ocorrer mais rapidamente.

- **OutbreakShield**: Com a OutbreakShield, é possível o reconhecimento e combate de pragas em e-mails em massa, antes que as assinaturas de vírus atualizadas estejam disponíveis. A OutbreakShield consulta na Internet sobre acumulações especiais de e-mails suspeitos e fecha, quase em tempo real, a brecha que existe entre o começo de um e-mail em massa e seu combate através de assinaturas de vírus adaptadas especialmente. Em **Alterar** , você pode definir se a OutbreakShield utilizará assinaturas adicionais a fim de aumentar a capacidade de reconhecimento. O carregamento das assinaturas pode estabelecer automaticamente a conexão à Internet. Além disso, é possível inserir dados de acesso para a conexão à Internet que possibilitam, ao OutbreakShield, o download automático de assinaturas da Internet.

Mensagens de aviso

Notificar usuário em caso de detecção de vírus: Você pode informar ao destinatário de uma mensagem infectada, automaticamente sobre esse fato. Para isso, será exibida uma mensagem de aviso em sua área de trabalho.

Proteção do Outlook

As seguintes funções estão disponíveis:

- **Proteger o Microsoft Outlook através de um plugin integrado**: Com a ativação desta função, será adicionada ao ***Outlook*** do cliente, no menu ***Ferramentas***, uma nova função com o nome ***Verificar a existência de vírus na pasta***. Independente das configurações do administrador, o usuário do cliente individual pode verificar a existência de vírus na pasta de correio desejada. Na janela de visualização de um e-mail, é possível, no menu ***Ferramentas***, através de ***Verificar a existência de vírus no e-mail*** , executar um controle de vírus nos anexos do arquivo. Após a conclusão do procedimento, aparece uma tela de informações na qual o resultado da verificação é resumido. Aqui você descobre se a análise de vírus ocorreu completamente, obtém informações sobre a quantidade de e-mails verificados, possíveis erros, assim como sobre os vírus detetados e como foi procedido com eles. Ambas as janelas podem ser ocultadas com um clique no botão ***Fechar*** .

- **Monitoramento de porta**: Em geral, são monitoradas as ***portas padrão*** para ***POP3***, ***IMAP*** e ***SMTP***. Se as configurações de porta do seu sistema forem diferentes, essas poderão ser adaptadas de acordo.

Web/Mensagens instantâneas

Aqui podem ser feitas as seguintes configurações.

Conteúdo da Internet (HTTP)

- **Processar conteúdo da Internet (HTTP)**: Nas opções da Web, você pode definir que a existência de vírus em todo o ***conteúdo da Web por HTTP*** seja verificada já na navegação. O conteúdo infectado da Web não é executado e as respectivas páginas não são exibidas. Para isso, coloque a marcação em **Processar conteúdo da Internet (HTTP)**.

- **Evitar ultrapassar limite de tempo no navegador**: Como o *G Data Software* processa o conteúdo da Web antes de sua exibição no navegador da Internet, e esse, dependendo dos resultados dos dados necessita de um certo tempo, pode ocorrer que um aviso de erro apareça no navegador da Web, pelo não recebimento imediato dos dados, devido a estarem sendo verificados. Com a colocação da marcação no campo **Evitar ultrapassar limite de tempo no navegador** , evita-se uma mensagem de erro e, assim que a existência de vírus for verificada em todos os dados do navegador, esses serão transmitidos normalmente para o navegador da Internet.

- **Limite de tamanho para downloads**: Através desta opção, é possível interromper uma verificação de HTTP para conteúdos da web muito grandes. O conteúdo é verificado pela sentinela de vírus assim que qualquer rotina maliciosa ficar ativa. A vantagem dessa limitação de tamanho é de que ao navegar na Web, nenhum retardo ocorre devido ao controle de vírus.

Mensagem instantânea

- **Processar conteúdo de mensagens instantâneas**: Como vírus e outros programas maliciosos podem ser propagados também através de ferramentas de mensagens instantâneas, o *G Data Software* pode impedir a exibição e o download de dados infectados em primeiro plano. Se na utilização de seus aplicativos de mensagens instantâneas você não usar as portas padrão, poderá informar em Número de porta de servidor, os respectivos ***endereços de portas***.

- **Mensagem instantâneas (Integração do aplicativo de mensagens instantâneas)**: Se você utilizar o ***Microsoft Messenger (a partir da Version 4.7)*** ou o ***Trillian (a partir da versão 3.0)***, é possível, colocando a marcação para o respectivo programa, definir um menu contextual no qual você poderá verificar a existência de vírus diretamente em arquivos suspeitos.

? Quando você não desejar a verificação de conteúdos da Internet, a **Sentinela de vírus** toma providências quando um arquivo infectado for inicializado. Ou seja, o sistema no respetivo cliente está protegido, mesmo sem a verificação do conteúdo da Internet, enquanto a sentinela estiver ativa.

AntiSpam

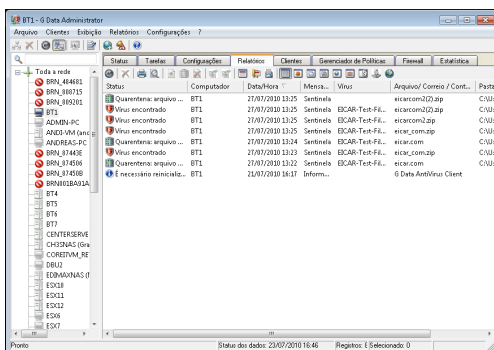
Aqui podem ser feitas as seguintes configurações.

Filtro de spam

Ao colocar a marcação em **Utilizar filtro de spam**, o tráfego de e-mail do cliente será verificado quanto a eventuais e-mails spam. Um aviso pode ser definido, que será exibido no assunto do e-mail, assim que um e-mail for reconhecido como Spam ou cair em suspeita de spam.

? Através do aviso, você ou o usuário podem definir uma regra no programa de e-mail cliente, de acordo com a qual, p.ex., os e-mails que tenham o aviso ***[Spam]***, na linha de assunto, sejam movidos automaticamente para a lixeira ou para uma pasta especial para e-mails spam e junk.

Relatórios

Todas as deteções de vírus são exibidas nessa área de tarefas. Na primeira coluna da lista, é exibido a área Status (p.ex, ***Vírus encontrado*** ou ***Arquivo movido para a quarentena***). Também é possível reagir a deteções de vírus; selecione os registros na lista e, em seguida, selecionando um comando no menu contextual (botão direito do mouse) ou na barra de ferramentas. Dessa forma, é possível excluir arquivos infectados ou mover para a ***pasta de quarentena*** .

Na área de tarefas **Relatórios** aparecem todos os relatórios sob os nomes designados por você e os mesmos podem ser organizados através de um clique na respetiva designação da coluna, por diferentes critérios. A coluna, de acordo com a qual a classificação atual é feita, é marcada através de uma pequena seta.

Estão disponíveis os seguintes critérios:

- **Status**: Aqui você obtém o conteúdo do respetivo relatório de forma breve e sucinta. Ícones significativos destacam a importância e o tipo de cada respetivo aviso.
- **Computador**: O computador do qual ocorreu o respetivo relatório será exibido aqui. Em grupos de usuários, cada computador é relacionado individualmente.
- **Data/Hora:**: A data na qual o relatório foi criado, devido a um vírus encontrado através da *Sentinela G Data* ou com base em uma tarefa de verificação.
- **Mensageiro:**: Através desse registro, você descobre se o relatório do ***Verificador de vírus*** ocorreu automaticamente através da ***Sentinela*** com base em uma tarefa de verificação ou informado através do *plugin de e-mail G Data*.
- **Vírus:**: Se conhecido, aqui será exibido o nome do vírus encontrado.

- **Arquivo/E-mail**: Aqui são relacionados os arquivos nos quais um vírus foi encontrado ou onde existe uma suspeita de vírus. No caso de ***e-Mails*** você encontra, adicionalmente, o endereço de e-mail do remetente.
- **Pasta**: As informações de diretório dos respetivos arquivos são importantes para o caso de um arquivo ser movido para a quarentena e, posteriormente, precisar ser movido de volta.

?

Na barra de menu, está disponível um registro adicional para a área de tarefas **Relatórios**. Para as funções que funcionam com arquivos (excluir, mover de volta e etc.), é preciso marcar o(s) respetivo(s) arquivo(s) na visão geral do relatório. Aqui se pode selecionar as seguintes funções:

- **Exibição**: Informe aqui se deseja que sejam exibidos todos os relatórios, apenas os relatórios sobre vírus não removidos ou apenas os da área de quarentena. Também é possível solicitar a exibição do conteúdo da área de quarentena.
- **Ocultar relatórios dependentes**: Quando, devido a diferentes tarefas ou tarefas executadas muitas vezes, uma mensagem de vírus ou um relatório forem exibidos diversas vezes, é possível ocultar a réplica aqui. Somente será exibido o registro mais recente, o qual poderá ser editado.
- **Ocultar arquivos em pastas compactadas**: Aqui é possível exibir ou ocultar avisos sobre relatórios e verificações de pastas compactadas. No caso de Detecção de vírus em uma pasta, o *G Data Software* cria, em geral, dois avisos, onde o primeiro informa que uma pasta compactada está infectada e o segundo informa o arquivo exato afetado NESSA pasta. Ao utilizar a função **Ocultar arquivos em pastas compactadas** ambos esses avisos são agrupados.

Quando você ***tiver configurado as*** tarefas de verificação em seu sistema, de tal forma que o ataque de vírus seja apenas registrado, será possível executar o combate ao vírus, também de forma manual. Selecione, para isso, no relatório, um ou mais arquivos registrados e execute a operação desejada através de:

- **Remover vírus do arquivo**: Tenta remover o vírus do arquivo original.
- **Mover arquivo para a quarentena**: Move o arquivo para a pasta de ***Quarentena***.
- **Excluir arquivo**: Exclui o arquivo original no cliente.

- **Quarentena: Limpar e mover de volta**: É feita uma tentativa para remover o vírus do arquivo. Quando isso é bem sucedido, o arquivo limpo é movido de volta para seu local de origem no respetivo cliente. Quando não for possível remover o vírus, o arquivo também não é movido de volta.
- **Quarentena: Mover de volta**: Move o arquivo da quarentena de volta ao cliente. ***Atenção***: O arquivo será restaurado em seu estado original e continuará infectado.
- **Quarentena: Enviar para a Internet Ambulance**: Se constatar um novo vírus ou um fenômeno desconhecido, envie-nos, por gentileza, em todos os casos, esse arquivo através da função de quarentena do *G Data Software*. Nós analisaremos o vírus e disponibilizaremos uma antídoto o mais rápido possível. Naturalmente, o nosso ***Serviço antivírus emergencial*** tratará os seus dados de forma altamente confidencial e discreta.
- **Excluir**: Exclui os relatórios selecionados. Quando for necessário excluir relatórios, aos quais um arquivo de quarentena pertence, essa exclusão terá que ser reconfirmada. Nesse caso, também serão excluídos os arquivos que se encontrarem na quarentena.
- **Excluir relatórios dependentes**: Quando, devido a diferentes tarefas ou tarefas executadas muitas vezes, uma mensagem de vírus ou um relatório forem exibidos em duplicidade ou diversas vezes, é possível excluir a réplica no arquivo de registro.

Atualizar

Essa função atualiza a visualização. Carrega os ***Relatórios*** atuais do ManagementServer.

Excluir relatórios

Através daqui, você exclui os relatórios selecionados. Quando tiver que excluir relatórios, dos quais um arquivo em ***Quarentena*** pertence, será preciso pressionar Excluir mais uma vez. Nesse caso, também serão excluídos os arquivos que se encontrarem na quarentena.

Imprimir

Através desta função, você inicia o processo de impressão para relatórios. Na janela que aparece, é possível definir os detalhes e as áreas que deseja imprimir.

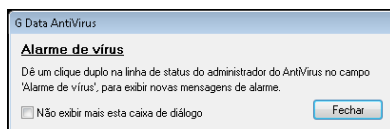
Visualizar página

Através da função Visualizar página, é possível antes da impressão em si, solicitar uma visualização da página a ser impressa, no monitor.

Remover vírus

Vom essa função você pode tentar remover o vírus manualmente do arquivo original. Na visão geral será exibido se a tentativa foi bem-sucedida.

Mover para a quarentena

Esta função move os arquivos selecionados para a pasta de quarentena. Os arquivos serão salvos codificados na pasta ***Quarentena*** no ManagementServer. Os arquivos originais serão excluídos. Através da codificação, é garantido que o vírus não possa causar nenhum dano. Observe que um relatório pertence a cada arquivo na quarentena. Se excluir o relatório, o arquivo também será excluído da pasta de quarentena. Você pode enviar um arquivo da pasta quarentena para verificação ao ***Serviço antivírus emergencial***. Para isso, dê um clique duplo no relatório de quarentena.

No diálogo do relatório, clique na entrada Motivo do envio, no botão **Enviar para a Internet Ambulance**.

Excluir arquivo

Com a função **Excluir arquivo**, você exclui o arquivo original do cliente.

Restaurar arquivo da quarentena

Através dessa opção, você move um arquivo da pasta ***Quarentena*** de volta para o cliente.

Atenção: O arquivo será restaurado em seu estado original e continuará infectado.

Limpar arquivo e restaurá-lo da quarentena

Com esta função, o vírus é removido do arquivo e o arquivo limpo será movido de volta ao cliente. Quando não for possível remover o vírus, o arquivo permanece na pasta ***Quarentena***.

Opções de exibição

No caso de uma grande quantidade de diferentes relatórios, é útil solicitar a exibição de acordo com diferentes critérios e em uma listagem. As seguintes possibilidades estão disponíveis:

Ocultar relatórios dependentes: Quando, devido a diferentes tarefas ou tarefas executadas muitas vezes, uma mensagem de vírus ou um relatório forem exibidos diversas vezes, é possível ocultar a réplica aqui. Somente será exibido o registro mais recente, o qual poderá ser editado.

Ocultar arquivos em pastas compactadas

Ocultar relatórios lidos

Exibir todos os relatórios

Exibir somente relatórios sobre vírus não removidos

 Exibir todos os relatórios da quarentena

 Exibir conteúdo da quarentena

 Exibir todos os relatórios de HTTP

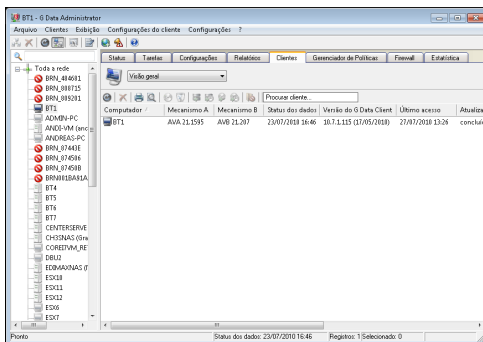
 Exibir todos os relatórios do firewall

 Exibir todos os relatórios do Controle de aplicativos

 Exibir todos os relatórios do Controle de dispositivos

 Exibir somente relatórios do controle de conteúdo da web

Clientes

Na ***área de Seleção de clientes*** selecione um grupo para obter a visão geral sobre todos os clientes do grupo. Para cada cliente, será exibido a versão dos componentes instalados e quando o cliente fez o login na última vez no ManagementServer. Aqui é possível facilmente verificar se os clientes estão funcionando corretamente e se as atualizações na Internet foram executadas.

Na área de tarefas **Clientes** estão disponíveis as seguintes informações em uma lista: Elas podem ser organizadas através de um clique na respetiva designação da coluna, por diversos critérios. A coluna, de acordo com a qual a classificação atual é feita, é marcada através de uma pequena seta. Estão disponíveis os seguintes critérios:

- **Computador**: Aqui é exibido o nome do respetivo cliente.
- **Mecanismo**: O número da versão do banco de dados de vírus e a data da última atualização por atualização da Internet são exibidos aqui.
- **Status dos dados:**: A data na qual o status do banco de dados de vírus foi atualizado no cliente. Essa data não é idêntica à data de atualização do banco de dados de vírus.
- **Versão do G Data Client**: Aqui você encontra o número da versão e a data da criação do software *G Data Client*.
- **Último acesso**: Através desse registro, você descobre em que momento o *G Data Client* esteve ativo pela última vez.
- **Atualização do banco de dados de vírus**: Aqui você descobre se a atualização do banco de dados de vírus está *concluída* se uma tarefa adicional foi atribuída ou se ocorreram irregularidades ou erros.
- **Atualização dos arquivos de programa**: Quanto novas atualizações tiverem que ser feitas no software cliente, você obtém, aqui, as respetivas informações de status.

- **Período**: A data na qual o status dos arquivos do programa foram atualizados no cliente.
- **Diretórios de exceções**: Contanto que você tenha criado diretórios de exceções que não devem ser considerados no controle de vírus para o respetivo cliente, serão exibidas ***as exceções*** aqui.

? Na barra de menu, está disponível um registro de menu adicional de nome **Clients** ein zusätzlicher Menüeintrag namens **Configurações do cliente** com as seguintes funções:

- **Instalar o G Data Client**: Instala o software cliente. A instalação só é possível quando o cliente atender a determinadas condições.
- **Desinstalar o G Data Client**: Atribui ao *G Data Client* a tarefa de se auto-desinstalar. Para a remoção completa, será preciso reiniciar o computador cliente. O usuário será solicitado a isso através de um aviso.
- **Instalar o G Data Client para Linux**: Também é possível instalar um software cliente especial em clientes Linux na rede. Para isto, leia o capítulo ***Leia para isso o capítulo Software cliente em computadores Linux*** no anexo desta documentação.
- **Atribuir o G data servidor de subrede**: Enquanto que com a função **Gerenciar o servidor** você tem a possibilidade de atribuir a determinados clientes ***Servidor de subrede***, através da função **Atribuir o G data servidor de subrede** também é possível selecionar, de forma objetiva, um servidor de subrede para o respetivo cliente.
- **Redefinir todas as configurações padrão**: Para a proteção de toda a rede ou de grupos selecionados ***, criar a configuração padrão*** e, com isso, rapidamente atribuir modelos para a proteção de vírus. Para colocar regras individuais para grupos individuais em um estado geral, é possível redefinir as configurações padrão com essa função para o valor padrão definido.
- **Atualizar banco de dados de vírus agora**: Atualiza os bancos de dados de vírus nos clientes com os arquivos do ManagementServer.
- **Atualizar banco de dados de vírus automaticamente**: Ativa a atualização automática do banco de dados de vírus. Os clientes verificam periodicamente se existe uma nova versão do ManagementServer e executam automaticamente a atualização.

- **Atualizar arquivos de programa agora**: Atualiza os arquivos de programa nos clientes com os arquivos do ManagementServer. Após a atualização dos arquivos de programa, pode ser que o cliente tenha que ser reiniciado.
- **Atualizar arquivos de programa automaticamente**: Ativa a atualização automática dos arquivos de programa. Os clientes verificam periodicamente se existe uma nova versão do ManagementServer e executam automaticamente a atualização.
- **Reiniciar após a atualização dos arquivos de programa**: Aqui, como administrador, é possível definir a prioridade que uma atualização dos arquivos de programa tem no cliente. Assim, através de **Abrir janela de observações no cliente**, é possível informar a um usuário que ele, em um momento adequado, deverá reiniciar o computador cliente, através de **Gerar relatório**, por meio dos arquivos de registro, na área **Relatórios** ele poderá executar manualmente ou **Reiniciar sem perguntar**.

Através da caixa de seleção localizada acima, é possível decidir se deseja editar uma **Visão geral** através do cliente ou se deseja enviar **Mensagens** aos clientes individuais. Com o envio dessas mensagens, é possível informar de forma rápida e descomplicada, ao usuário, alterações no status do cliente que esses utilizam.

Visão geral

Aqui você obtém uma visão geral sobre todos os clientes administrados, podendo administrá-los também simultaneamente.

Atualizar

Essa função atualiza a visualização e carrega as configurações atuais do cliente do ManagementServer.

Excluir

Através deste, você remove um cliente de um ***grupo***.

Imprimir

Através desta função, você inicia o processo de impressão das configurações do cliente. Na janela que aparece, é possível definir os detalhes e as áreas das configurações do cliente que deseja imprimir.

Visualizar página

Aqui, antes da impressão, é possível solicitar uma visualização da página a ser impressa no monitor.

Instalar o G Data Client

Instala o *software do G Data Client*. A instalação só é possível quando o cliente atender a determinadas condições.

Você pode equipar os clientes do ***ManagementServer*** com o *software G Data Client*, contanto que esses atendam a determinadas condições. Com a ativação dessa função, é aberto um menu, no qual são inseridos os dados de acesso para o servidor, através do qual deverá ocorrer a instalação do *G Data Client*.

Após a inserção dos respetivos dados (que são armazenados pelo programa e, portanto, não precisam novamente ser inseridos), confirme com **OK**. Em seguida, é aberta uma caixa de diálogo na qual são exibidos todos os clientes disponíveis. Selecione aqui um ou mais clientes desativados e clique, em seguida, em **Instalar**. O *G Data Software* instala automaticamente o software cliente no respetivo computador. Se a instalação do software não for possível através da ***Instalação remota*** descrita aqui, essa poderá ser instalada manualmente ou de forma semiautomática nos clientes.

? Para ser possível acessar ***clientes desativados***, esses deverão também ser exibidos na visualização de diretório. Na utilização da função **Instalar Cliente G Data**, o programa informa isso, se necessário, e possibilita uma apresentação do cliente desativado.

? Também é possível instalar um software cliente especial em ***clientes Linux*** na rede. Para isto, leia o capítulo ***Leia para isso o capítulo Software cliente em computadores Linux*** no anexo desta documentação.

? Na instalação do software cliente, você será perguntado se o ***G Data Firewall*** deverá também ser instalado em conjunto no computador cliente. Mais informações sobre o ***Firewall*** podem ser obtidas no capítulo de mesmo nome desta documentação.

Desinstalar o G Data Client

Atribui ao *G Data Client* a tarefa de se auto-desinstalar. Para a remoção completa, será preciso reiniciar o cliente. O usuário será solicitado a isso através de um aviso.

Atualizar banco de dados de vírus

Atualiza o banco de dados de vírus no cliente com os arquivos do ManagementServer.

Atualizar banco de dados de vírus automaticamente

Ativa a ***atualização automática do banco de dados de vírus***. Os clientes verificam periodicamente se existe uma nova versão do ManagementServer e executam automaticamente a atualização.

Atualizar arquivos de programa

Atualiza os arquivos de programa no cliente com os arquivos do ManagementServer. Após a atualização dos arquivos de programa, pode ser que o cliente tenha que ser reiniciado.

Atualizar arquivos de programa automaticamente

Ativa a atualização automática dos arquivos de programa. Os clientes verificam periodicamente se existe uma nova versão do ManagementServer e executam automaticamente a atualização.

Editar diretório de exceções

Aqui é possível definir diretórios de exceção para os clientes, os quais não deverão ser verificados durante a execução de tarefas de verificação.

Mensagens

Como administrador, você pode enviar mensagens a clientes individuais ou grupos **Mensagens**. Com o envio dessas mensagens, você pode informar, aos usuários, alterações no status dos clientes que eles utilizam. As mensagens serão exibidas como informações na barra de ferramentas do computador cliente.

Para criar outras mensagens, basta clicar no botão **Novo**. No diálogo que aparece, você pode marcar ou desmarcar os clientes aos quais deseja enviar mensagens! Digite no campo **Mensagem** suas instruções para os respetivos clientes e pressione o botão **Enviar**.

? Se deseja tornar uma mensagem acessível somente a determinados usuários de um computador cliente ou rede, insira o nome de login do mesmo em **Nome de usuário**.

Gerenciador de Políticas

O PolicyManager é um controle individual de dispositivos, aplicativos e da Internet, assim como um filtro de conteúdo para garantir a política da sua empresa no local de trabalho. Você determina que usuários têm que direitos, define as possibilidades de acesso, liberação e muito mais. Você determina quem quando e onde navega e impede pen drives e programas indesejados. Através da caixa de seleção localizada acima, é possível decidir que tipo de configurações de segurança você deseja editar através dela.

Através do botão **Configurações** você pode ativar ou desativar diferentes opções de notificação. Se colocar aqui a respectiva marcação, o usuário pode perguntar ao administrador no respectivo computador cliente, através de um diálogo na bandeja, se aplicativos, dispositivos ou conteúdos da web podem ser liberados para ele. Se a marcação não estiver colocada, essa caixa de diálogo interativo não existirá.

Controle de aplicativos

Com o Controle de aplicativos, é possível bloquear determinados programas, arquivos e pastas para a utilização através de determinados clientes. Para isso, determine em **Status** se as restrições deverão valer para todos os usuários do respetivo cliente ou apenas para usuários que não tenham direitos de administrador no computador do cliente. Em Modo, você define se, na lista de controle de aplicativos, deverá tratar-se de uma Whitelist ou Blacklist.

- **Whitelist**: Somente os aplicativos, arquivos e pastas aqui relacionados podem ser utilizados pelo computador cliente.
- **Blacklist**: Os aplicativos aqui relacionados não podem ser utilizados no computador do cliente.

Criar novas regras

Clique no botão **Novo** para definir uma nova regra. Você tem a opção entre os tipos de regra **Fabricante**, **Arquivo** e **Diretório**.

- **Fabricante**: Aqui são utilizadas as informações do fabricante nos arquivos de programa para permitir ou proibir uma utilização desse aplicativo. O nome do fabricante pode ser inserido aqui por você ou, através do botão com três pontos, selecionar objetivamente um arquivo a partir do qual as informações do fabricante serão lidas e aplicadas.
- **Arquivo**: Aqui é possível bloquear ou permitir determinados arquivos de programa para o respetivo cliente. Para isso, você pode inserir o nome do arquivo e proibir ou permitir o acesso geral a arquivos com esse nome, ou clicar no botão **Determinar as características de um arquivo** para definir um determinado arquivo de forma especial através de suas características. Em caso de necessidade, você pode utilizar como espaço reservado para conteúdos desejados, um (*) no início e/ou final do nome do arquivo de característica, nome do produto e copyright.
- **Diretório**: Através dessa função, você pode liberar ou bloquear diretórios completos (se desejado, inclusive os respectivos subdiretórios) para clientes.

Controle de dispositivos

Com a ajuda do controle de dispositivos, é possível definir os clientes que têm acesso a dispositivos periféricos especiais. Dessa forma, é possível evitar a utilização de pen drives, equipar unidades de CD com direitos de gravação ou leitura e também restringir a utilização de câmeras ou outros periféricos.

> **?** Em **Status** é possível definir se as restrições deverão valer para todos os usuários do respetivo cliente ou apenas para usuários que não tenham direitos de administrador no computador do cliente.

Para cada cliente, será eixibido abaixo de **Dispositivos** os que podem ser bloqueados. Esses não precisam necessariamente estar disponíveis também no respetivo cliente, ou seja, por exemplo, você pode impedir em geral para um grupo de usuários selecionados, a utilização de disquetes, independente se os respecivos computadores têm uma unidade de disquete ou não.

As seguintes permissões podem ser definidas:

Leitura/Gravação: Permite o total acesso ao dispositivo periférico.

Ler: As mídias só podem ser lidas, não é possível a gravação de dados.

Proibir acesso: O acesso à leitura e à gravação não são permitidos no dispositivo. O dispositivo não pode ser utilizado pelo usuário.

Whitelist

Através das configurações da Whitelist, você pode permitir novamente a utilização do dispositivo que restringiu de alguma forma para o usuário do cliente (proibir**Leitura** / **Acesso**) com determinadas restrições. Se clicar no botão **Novo**, é aberto uma janela de diálogo na qual os dispositivos são exibidos com as restrições de utilização. Se clicar agora em**ID do hardware/ID da mídia:** poderá permitir uma exceção para determinados dispositivos.

- **Utilizar ID da mídia**: Aqui é possível definir que somente determinados CDs ou DVDs possam ser utilizados com uma unidade de CD/DVD, p. ex, apresentações especiais da empresa em CD ou algo do gênero.
- **Utilizar ID do hardware**: Aqui é possível definir que somente determinados pen drives possam ser utilizados. Com uma ID de hardware, você tem, por exemplo, uma visão geral sobre quais funcionários têm a possibilidade de repassar dados.

? Para determinar uma ID de mídia ou de hardware, vá para o diálogo **Determinar ID do hardware/ID da mídia** no registro **Cliente** e lá selecione o cliente no qual a mídia ou hardware a ser liberado se encontra. A respectiva ID será lida automaticamente.

Através da procura local, é possível determinar a ID da mídia ou do hardware a partir do computador com o qual você administra a rede.

Controle de conteúdo da web

O controle de conteúdo da web serve para permitir aos usuários o acesso à Internet durante o serviço, mas não a navegação em sites indesejados ou para impedir determinadas áreas de tópicos. Após a seleção do cliente a ser editado na parte direita da interface do programa, você poderá objetivamente permitir o respectivo cliente através de uma marcação ou proibir removendo a marcação em determinadas áreas.

As categorias abrangem uma grande quantidade de áreas temáticas e são atualizadas constantemente pela G Data e mantidas dessa forma. Como administrador, você não terá mais o trabalho de cuidar disso, assim que as respectivas liberações ou restrições estiverem definidas para o cliente.

? Em **Status** é possível definir se as restrições deverão valer para todos os usuários do respetivo cliente ou apenas para usuários que não tenham direitos de administrador no computador do cliente.

Whitelist

Com a **Whitelist** você pode - independentemente das configurações feitas em **Categorias permitidas** - cuidar para que determinados sites ou URLs sejam permitidos para toda a rede. Isso pode, p.ex., ser a presença na web da sua empresa. Para isso, basta inserir os endereços que deseja liberar em **URLs**, clicar depois no botão **Adicionar** e a respectiva página estará liberada.

Blacklist

Com a **Blacklist** , você pode - independentemente das configurações feitas em **Categorias permitidas** - cuidar para que determinados sites ou URLs sejam bloqueados para toda a rede. Quando você permite, em geral, a utilização da Internet em sua empresa, isso pode, p.ex., ser feito a sites da web que não são desejados devido a uma grande quantidade de dados, como portais de vídeo. Para bloquear, basta inserir em **URLs** o endereço que deseja bloquear, em seguida, clique no botão **Adicionar** e o respectivo site estará bloqueado por toda a empresa.

Monitorar tempo de utilização da Internet (atividade de fato na Internet)

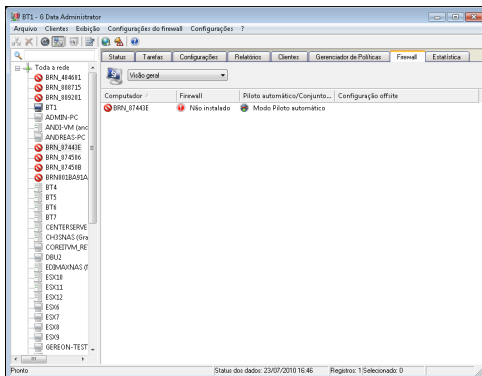
Através das informações na área **Horários de utilização** , é possível restringir a utilização privada ou geral da Internet para determinados períodos ou contingentes de tempo. Para restringir o tempo de utilização individual na Internet, primeiro selecione os grupos ou clientes que deseja editar. Agora, em **Status** , determine se as restrições deverão valer para todos os usuários do respetivo cliente ou apenas para usuários que não tenham direitos de administrador no computador do cliente. Depois disso, você pode definir quanto tempo o usuário pode usar a Internet no total por mês, quanto tempo por semana e quantas horas em determinados dias da semana. Dessa forma, os fins de semana podem ter tratamento diferente dos dias da semana para os usuários. Os respectivos períodos podem ser inseridos para isso em **Dias/hh:mm**, onde, por exemplo, uma entrada ***04/20:05*** daria um tempo de utilização de 4 dias, 20 horas e 5 minutos na Internet.

? Em relação aos dados para a utilização da Internet, contam sempre respectivamente, os valores menores. Então, se você definir para o mês uma restrição de tempo de quatro dias, mas permitir na semana cinco dias, o software reduz a utilização do usuário automaticamente para quatro dias na Internet.

Quando o respectivo usuário tentar acessar a Internet acima do contingente de tempo, aparece uma tela de informações no navegador, que informa que seu contingente foi ultrapassado.

Na área **Horários de bloqueio** você pode, adicionalmente à restrição quantitativa da utilização da Internet, bloquear períodos especiais na semana de forma categórica. Períodos bloqueados são representados em vermelho e os liberados em verde. Para liberar ou bloquear um período, basta marcá-lo com o mouse. Em seguida, aparecerá ao lado do cursor do mouse, um menu contextual onde você terá duas possibilidades: **Liberar período** e **Bloquear período**. Quando o respectivo usuário tentar acessar a Internet durante os períodos bloqueados, aparece uma tela de informações no navegador, que o informa que nesse período, ele não tem direito ao acesso à Internet.

Firewall

Através desta área, você pode administrar o firewall nos respetivos clientes ou centrado nos grupos. Através da caixa de seleção acima, é possível decidir se deseja administrar uma visão geral sobre o status do firewall do respetivo e-mail do cliente ou definir conjuntos de regras.

Visão geral

Na visão geral, são exibidos todos os computadores clientes ou os clientes de um grupo selecionado. Aqui você vê, de uma vez, quais configurações o respetivo firewall do cliente tem e pode, através do clique no respetivo cliente, realizar alterações diretamente.

> **?** ***Conjunto de regras ou piloto automático?***
> Existem duas possibilidades básicas para utilizar um firewall.
>
> - **Piloto automático**: Quando o firewall é utilizado no modo "Piloto automático", ele já é pré-configurado, por padrão, pela ***G Data***, cumpre com suas tarefas em segundo plano e não incomoda o usuário com perguntas, com as quais ele se otimiza crescentemente com o aprendizado.
> - **Conjunto de regras**: Como administrador, você pode definir regras especiais para o firewall para diferentes ambientes de computadores; assim, por exemplo, é possível definir conjuntos de regras para a conexão direta com a Internet, redes confiáveis ou não, ou também outros ambientes.

As seguintes informações são disponibilizadas pela visão geral:

- **Computador**: O nome do computador cliente. Por meio dos ícones ilustrados, você pode reconhecer aqui se o software cliente está instalado nesse cliente.
- **Firewall**: Aqui você descobre se o firewall está ativado, desativado ou até mesmo não instalado no cliente.
- **Piloto automático/Conjunto de regras**: Você pode atribuir, a diferentes clientes, diferentes funcionalidades do firewall. Desde o Modo Piloto automático amigável ao usuário até os Conjunto de regras definidos individualmente.
- **Configuração offsite**: Se optar pela configuração offsite para um cliente, o usuário pode administrar e configurar individualmente suas configurações do firewall nesse cliente, enquanto ele não estiver conectado á rede do ManagementServers. A configuração offsite só pode ser utilizada quando o firewall não for utilizado no modo Piloto automático na rede empresarial.

Para alterar as configurações do firewall para os clientes selecionados na lista, clique no registro com o botão direito do mouse. É aberto um menu de seleção com as seguintes opções:

- **Configurações**: Através dessa janela de diálogo, é possível efetuar configurações básicas para o respetivo firewall cliente. Para isto, leia o capítulo **Configurações do firewall**.
- **Criar conjunto de regras**: Através daqui, você alterna para a área **Conjunto de regras** e pode definir regras individuais para o firewall de seu cliente.
- **Editar conjunto de regras**: Através daqui, você alterna para a área **Conjunto de regras** e pode definir regras existentes para o firewall de seu cliente.
- **Selecionar conjunto de regras**: Aqui é aberto um diálogo, no qual é possível selecionar ***conjuntos de regras*** já definidos ou também ativar o modo ***Piloto automático*** para o respetivo firewall do cliente.
- **Instalar firewall**: Através desta função, você pode instalar de forma central um firewall e, em seguida, também administrá-lo.
- **Desinstalar firewall**: Com essa função, o firewall do cliente, existente, é desinstalado.

Configurações do firewall

Na janela de diálogo para as configurações do firewall, é possível efetuar definições básicas para a funcionalidade do respetivo cliente do firewall:

- **Firewall ativado**: Através da colocação da marcação, o firewall é ativado no respetivo cliente. Se você remover a marcação, o firewall ficará ativo.

- **Informar sobre aplicativos bloqueados**: Quando essa marcação é colocada e o computador cliente estiver conectado ao ManagementServer, o Administrator recebe na área **Relatórios** informações sobre aplicativos que foram bloqueados através do respetivo firewall do cliente.

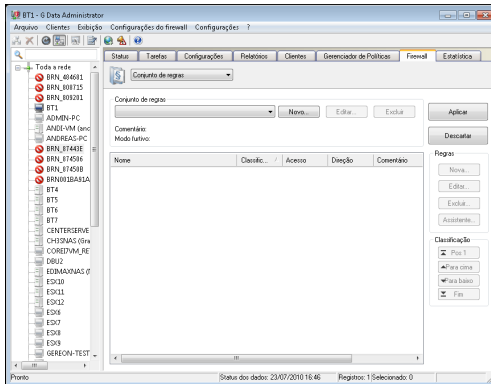
- **O usuário pode ativar e desativar o firewall**: Aqui, como administrador, você pode permitir que o usuário do computador cliente desative o firewall temporariamente. Essa possibilidade só é oferecida enquanto o cliente se encontrar dentro da rede da empresa, e só deve ser possibilitada a usuários avançados.

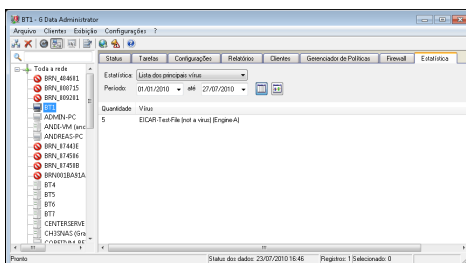
- **Utilizar configurações offsite para clientes móveis**: Na ***Configuração offsite***, os conjuntos de regra do firewall do computador cliente que valem na rede de sua empresa são substituídos por conjuntos de regras padrão, os quais regulam automaticamente o trato com a Internet, redes seguras e as não protegidas, além de redes a serem bloqueadas. Dessa forma, o computador móvel é protegido de forma ideal, enquanto ele não estiver na rede do ManagementServer. Assim que o computador móvel for novamente conectado à rede do ManagementServers, esses conjuntos de regras padrão são automaticamente substituídos pelos conjuntos de regras, como os válidos para o respetivo cliente em sua rede.

- **O usuário pode alterar as configurações offsite**: Essa opção permitirá que usuários avançados configurem seu firewall, individualmente, fora da rede. Assim que o computador móvel for novamente conectado ao ManagementServer, as alterações executadas serão substituídas pelas predefinidas pelo administrador para esse cliente.

? A ***configuração offsite*** só pode ser utilizada quando o firewall não for utilizado no ***Modo Piloto automático*** na rede empresarial. Quando o respetivo cliente utilizar as configurações do Piloto automático para o firewall, elas serão também utilizadas quando o cliente não estiver conectado à rede.

Conjunto de regras

Na área **Conjunto de regras**, você pode determinar regras de firewall individuais para todas as necessidades e áreas de sua rede. Informações detalhadas sobre como criar regras, administrá-las e utilizá-las podem ser encontradas na documentação sobre o uso do firewall.

Estatística

Nesta área de tarefas, é possível solicitar a exibição de informações estatísticas sobre o surgimento de vírus e infecções em seus clientes. Para isso, basta selecionar em **Estatística** se deseja uma visão geral sobre os clientes e suas interações com o ManagementServer (**Visão geral dos clientes**), uma visão geral sobre os vírus combatidos (**Lista dos principais vírus**) ou uma listagem com os clientes infectados (**Lista dos clientes infectados**).

G Data Client

O ***software Cliente*** disponibiliza a proteção antivírus para os clientes e executa as tarefas do ManagementServer sem a interface do usuário em segundo plano. Os clientes dispõem de assinaturas de vírus próprias e um próprio agendador, para que seja possível executar análises de vírus também no modo offline (p.ex., para Notebooks).

Instalação do cliente

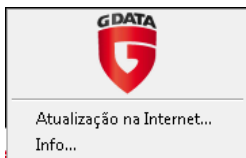
O ***software Cliente*** disponibiliza a proteção antivírus para os clientes e executa as tarefas do ManagementServer sem a interface do usuário em segundo plano. A instalação do software cliente ocorre, normalmente, centralizando todos os clientes através do Administrator. Através daqui, você será guiado no Administratortool por um Assistente de instalação.

Se a instalação do cliente falhar através da rede, o software cliente pode também ser instalado diretamente nos computadores cliente. Para a instalação do cliente em um computador cliente, insira o *CD-ROM G Data* na unidade de CD-ROM do computador cliente e pressione o botão **Instalar**. Em seguida, selecione o componente **G Data Client** com um clique no botão ao lado. Durante o andamento da instalação, informe o ***Nome do servidor*** ou o ***Endereço IP do servidor*** no qual o ManagementServer está instalado. O nome do servidor é necessário para que o cliente possa fazer contato com o servidor através da rede. Além disso, é necessário inserir o ***nome do computador*** do mesmo, se não for exibido automaticamente.

? Para a instalação de clientes para o servidor de arquivos Samba, leia no anexo desta documentação, o capítulo: ***Instalação do cliente para servidor de arquivos Samba.***

Ícone da segurança

Após a instalação do software cliente, é disponibilizado ao usuário do cliente, um ícone na barra Iniciar, através do qual esse, independente de predefinições administrativas, pode também verificar de forma independente o sistema quanto à infecção ou vírus.

Através do ***botão direito do mouse*** ele pode, nesse *ícone do G Data Client*, abrir um ***menu contextual*** que possibilita as seguintes funiconalidades:

Verificação de vírus

Através desta funcionalidade, o usuário pode, objetivamente, com o *G Data Client,*verificar a existência de vírus em seu computador fora dos períodos predeterminados pelo Administrator. Da mesma forma, o usuário pode, aqui, controlar CD-ROMs, memória e área de inicialização automática, assim como arquivos individuais ou diretórios (pasta) de forma objetiva. Dessa forma, usuários de notebook podem também impedir infecções por vírus em seus computadores que raramente são conectados à rede da empresa. Além disso, agora ele tem a possibilidade de mover arquivos infectados localmente para a pasta de quarentena, tornando-os inofensivos e disponibilizando-os para avaliação do administrador da rede, na próxima oportunidade.

? O usuário pode, a partir do Explorer, verificar arquivos ou diretórios de forma simples, marcando-os com o botão direito do mouse e, em seguida, no ***menu contextual***, utilizando a função **Verificar a existência de vírus (G Data AntiVirus)**.

Durante uma verificação de vírus em execução, o menu contextual pode ser ampliado com os seguintes registros:

- **Verificação de vírus prioritária**: O usuário tem aqui a possibilidade de determinar a prioridade da verificação de vírus. Em ***Alta***, a verificação de vírus é feita rapidamente, mas ela pode tornar o trabalho com outros arquivos bem mais lentos nesse computador. Na configuração ***Baixa***, a verificação de vírus é comparavelmente mais lenta, mas pode-se trabalhar sem maiores restrições no computador cliente.
- **Interromper verificação de vírus**: Através dessa opção, o usuário pode interromper a verificação de vírus e recomeçá-la posteriormente.
- **Cancelar verificação de vírus**: Enquanto o administrador mantiver a opção, **o usuário pode alterar as opções de sentinela**, um usuário pode interromper o controle de vírus no cliente também, mesmo quando a verificação foi iniciada manualmente nele.
- **Exibir janela de verificação**: Através dessa, o usuário pode solicitar a exibição da janela de informações, na qual aparecem andamento e progresso da verificação de vírus.

Desativar sentinela

Através desse comando, a *G Data Sentinela* pode ser desativada pelo usuário por um período determinado (de ***5 minutos*** até ***a próxima reinicialização do computador***). Naturalmente, isso só é possível quando o usuário tiver recebido os direitos correspondentes. A desativação temporária da sentinela, pode ser útil p.ex., em processos abrangentes de cópia de arquivos, porque dessa forma, o processo de cópia será acelerado. No entanto, o controle de vírus estará desativado nesse período. Aqui é preciso ponderar.

Opções

Contanto que o administrador tenha ativado a opção **O usuário pode alterar as opções da sentinela**, o usuário pode adaptar, no cliente, as opções para a verificação de vírus e seu computador, assim como as opções para a sentinela executada em segundo plano, também a suas necessidades pessoais.

? ***Atenção***: Dessa forma, naturalmente, todos os mecanismos de controle de vírus podem ser praticamente desativados no cliente. Como administrador, essa opção só deve ser disponibilizada a usuários tecnicamente avançados.

? As configurações relevantes à segurança, em **Opções**, também podem ser protegidas por senha para o computador cliente. Para isso, o administrador atribui para o respetivo cliente uma senha individual, com a qual o usuário pode alterar as funções de controle de vírus no cliente. Essa senha será atribuída através da área de trabalho **Configurações** no Administrator em **Proteção por senha para alterações de opções** .

As possibilidades de configuração individuais, que estão disponíveis ao usuário através da área **Opções** , são explicadas detalhadamente na área ***Estrutura do programa do Administrador > Área de tarefas> Configurações***, nos seguintes capítulos:

- **Sentinela**
- **E-Mail**
- **Verificação de vírus**
- **Filtro da Web/IM**
- **Filtro de spam**

? Quando você ativa para o usuário, no seu cliente, a opção **O usuário pode executar ele mesmo as atualizações de vírus** , ele poderá, independente do controle de vírus automático da sentinela, verificar seu computador cliente quanto à existência de vírus. As configurações possíveis aqui para o usuário no cliente correspondem praticamente às encontradas também na **Sentinela** .

Quarentena

Mesmo para computadores que não estão conectados à rede monitorada da *G Data* , existe uma pasta de quarentena local disponível. Dessa forma, usuários que estejam fora do local (p.ex., durante uma viagem de negócios) podem mover arquivos suspeitos para a quarentena e deixar que sejam avaliados na próxima oportunidade na rede da empresa. Na pasta quarentena, é possível desinfectar arquivos infectados; quando isso não funcionar, excluí-los e, se necessário, restaurá-los da quarentena para seu local de origem.

? ***Atenção***: Na restauração, o vírus não terá sido removido. Você só deve selecionar essa opção quando o programa não funcionar sem o arquivo afetado e você, mesmo assim, precisar dele para salvar dados.

Atualização na Internet

Através do *G Data Client* , também é possível executar atualizações das assinaturas de vírus na Internet, de forma independente, a partir do computador cliente. Isso é útil, por exemplo, em notebooks que periodicamente não têm acesso à rede da empresa. Essa funcionalidade também pode ser explicitamente liberada para clientes individuais pelo Administrator.

? Através do botão **Configurações e Programação** , também é possível realizar a atualização de assinaturas de vírus controlada a partir do cliente.

Firewall

Através da área do firewall, os usuários podem efetuar configurações abrangentes para o firewall de seu cliente, quando essa opção para o respetivo cliente tiver sido liberada do lado do servidor. Enquanto o cliente encontrar-se na rede do ManagementServer, o firewall será administrado de forma central a partir do servidor. Informações detalhadas sobre a funcionalidade desse firewall podem ser obtidas no capítulo ***Firewall***.

Informações

Através de **Informações**, é possível descobrir a versão da atualidade do banco de dados de vírus.

G Data WebAdministrator

O *G Data WebAdministrator* é um software de controle, baseado na web, para o ManagementServer. Ele pode ser iniciado por meio de um ***navegador da Internet***.

Instalação do WebAdministrator

O ***WebAdministrator*** é um software de controle, baseado na web, para o ManagementServer. Ele pode ser iniciado por meio de um navegador da Internet. Na instalação do WebAdministrator , você poderá ser solicitado a instalar ***componentes da Microsoft .NET Framework***. Esses são imprescindíveis ao funcionamento do WebAdministrator. Após a instalação, é necessário reinicializar.

? ***Atenção***: ANTES da instalação do WebAdministrator, é necessária a ativação da função do Windows ***Compatibilidade com a metabase IIS e Configuração IIS 6***. Se essa função não estiver disponível, a instalação do WebAdministrator será cancelada. Esse registro pode ser encontrado, p.ex., no Windows Vista em ***Iniciar > Painel de Controle > Programas > Programas e Recursos > Ativar ou Desativar Recursos do Windows***. Aqui você pode ativar o registro em ***Serviços de Informação da Internet > Ferramentas de Administração da web > Compatibilidade com a metabase IIS 6 > Compatibilidade com a metabase IIS e Configuração IIS 6***. Além disso, caso ainda não esteja, o ***Serviço WWW*** precisa estar ativado. Para isso, coloque a marcação em ***Serviços de informação da Internet > Serviço WWW***.

Agora será possível instalar o WebAdministrator.

Após a instalação, aparece, na área de trabalho de seu computador, o ícone para o ***G Data WebAdministrator*** .

Estrutura do programa WebAdministrator

Para utilizar o ***WebAdministrator***, basta clicar no ícone da área de trabalho do WebAdministrator. O seu navegador da web abrirá automaticamente com a página de login para acesso ao WebAdministrator. Insira aqui, como no ***Administrador*** normal, os seus ***Dados de acesso*** e clique no botão **Registrar**. A funcionalidade do WebAdministrator corresponde, tanto no conteúdo como também na utilização, praticamente a do ***G Data Administrator*** normal.

Firewall

Um firewall protege o seu computador contra a espionagem. Ele verifica que dados e programas da Internet ou rede, chegam em seu computador e que dados são enviados pelo seu computador. Assim que algo indicar que os dados em seu computador foram reproduzidos ou descarregados indevidamente, o firewall dá um alarme e bloqueia a troca de dados indevida. Por via de regra, é útil utilizar o Firewall no ***Modo Piloto automático***. Ele rodará praticamente em segundo plano e o protegerá, sem a necessidade de grandes configurações.

? Quando o Firewall é utilizado no ***Modo Piloto automático***, ele permanece completo em segundo plano e funciona de forma independente. Quando o Firewall é utilizado de forma ***definida pelo usuário***, em caso de dúvidas, aparece uma janela de diálogo na qual é possível otimizá-lo aos poucos de acordo com as situações. O Modo Piloto automático é padrão na instalação do Firewall.

Assim que estiver instalado, o firewall monitora todas as atividades de rede do seu computador. Quando você trabalha localmente com o seu computador, o firewall só aparece através do ***Ícone da segurança*** na barra Iniciar do Windows. Informações sobre as funções individuais com possibilidade de serem abertas através do ícone de segurança podem ser lidas no capítulo **Ícone da segurança**

Através dos botões **Configurar** e **Avançado(a)**, você pode configurar o firewall individualmente, se não desejar utilizar o modo piloto automático.

Configurar

Em geral, o firewall roda no modo Piloto automático. Somente com conhecimentos avançados no trato com redes, acessos à Internet e transferência de dados, é recomendável alterar as configurações do firewall. Se desejar adaptar individualmente as configurações do firewall, poderá fazê-lo através da interface do programa firewall. Com o auxílio de diferentes guias que podem ser selecionadas por meio dos ícones exibidos à esquerda no firewall, você alterna para a respectiva área do programa e lá pode executar ações, informar predefinições ou verificar processos.

Status

Na área de status do Firewall, você obtém informações básicas sobre a situação atual do seu sistema e do Firewall. Essas podem ser encontradas à direita do respectivo registro como informações em texto ou número. Além disso, o status do componente é indicado graficamente. Com um clique duplo no respectivo registro (ou, através da seleção do registro e um clique no botão **Edita**) você pode tomar providências diretamente aqui ou alternar para a respectiva área do programa. Assim que tiver otimizado as configurações de um componente com o ícone de aviso, o ícone na área de status torna-se novamente verde.

- **Segurança**: Enquanto você utiliza o computador para o seu trabalho diário, o Firewall aprende cada vez mais que programas você utiliza para o acesso à Internet e que programas são ou não um risco para a segurança. Dependendo do seu nível de conhecimento sobre o assunto tecnologia de firewall, poderá configurar o seu firewall de forma que ele ofereça uma muito boa proteção básica sem fazer perguntas demais, ou uma proteção profissional que se adapte ao seu comportamento de utilização do computador, mas que requeira de sua parte alguns conhecimentos como usuário. Um clique duplo do mouse no registro **Segurança** e você terá uma opção entre as seguintes Variações de segurança:

  Modo Piloto automático (recomendado): Aqui o Firewall trabalha de forma totalmente autônoma e evita os perigos automaticamente de PCs residenciais. Essa configuração oferece uma proteção geral prática e é, na maioria dos casos, recomendável.

  Criação manual de regras: Se desejar configurar o seu Firewall de forma individual ou não desejar que determinados aplicativos não trabalhem junto com o Piloto automático, poderá ajustar a sua proteção de Firewall através da criação manual de regras totalmente às suas necessidades pessoais.

- **Modo**: Aqui você será informado sobre as configurações básicas de acordo com as quais o Firewall está sendo utilizado. As possibilidades aqui são a Criação manual de regras ou o Automático (***Piloto automático***).

- **Rede**: O Firewall monitora naturalmente todas as atividades da rede, como p.ex., uma ***rede dial-up*** e uma ***conexão LAN***. Se uma ou mais redes não tiverem que ser protegidas, porque p.ex., foram definidas manualmente como exceção do monitoramento do Firewall, isso é indicado por um ícone de aviso. Um clique duplo no respectivo registro abre uma janela de diálogo, através da qual é possível configurar individualmente regras e definições para a rede selecionada. Em **Conjunto de regras**, selecione se a respectiva rede deverá fazer parte das ***redes confiáveis***, das ***redes não confiáveis*** ou das ***redes a serem bloqueadas***.

? A configuração **conexão direta com a Internet** se orienta ao máximo possível nas configurações válidas também para ***redes confiáveis***.

? A cada ***rede*** é possível atribuir um ***Conjunto de regras*** especial. Na área **Redes**, você vê as redes existentes no seu computador, enquanto que na área **Conj. de regras**, você vê quais os conjuntos de regras automáticos ou criados por você estão disponíveis no Firewall.

- **Ataques registrados**: Assim que o Firewall registra um ataque ao seu computador, esse será registrado aqui e será possível obter informações mais detalhadas clicando no item do menu.
- **Radar de aplicativos**: O Radar de Aplicativos exibe os programas que estão sendo bloqueados pelo Firewall no momento. Se você desejar permitir que os aplicativos bloqueados acessem a rede, basta selecioná-los e clicar no botão **Permitir**.

Redes

Na Área de redes são listadas as redes (p.ex., ***LAN***, ***Rede de transmissão de dados remotos*** e etc.) com as quais o seu computador está conectado. Aqui também será exibido o ***conjunto de regras*** de acordo com o qual (consulte o capítulo **Conjunto de regras**) a respectiva rede será protegida. Se você remover a marcação da respectiva rede, essa será retirada da proteção do firewall. No entanto, você só deve desativar a proteção em casos específicos isolados. Se você marcar a rede com o mouse e clicar no botão **Editar**, você poderá ver ou alterar as configurações de firewall para essa rede.

Editar rede

Na edição das configurações de rede existe a opção de utilizar o ***Assistente de regras*** ou a ***Caixa de diálogo avançada***. Em geral, recomenda-se a utilização do Assistente de regras porque esse ajudará o usuário na criação de regras e configurações.

- **Informações sobre a rede**: Aqui você obtém informações sobre a rede e, se existirem, dados sobre o ***Endereço IP***, ***Máscara de sub-rede***, ***Gateway padrão***, ***servidor DNS*** e ***WINS***.
- **Firewall ativo nessa rede**: Aqui você pode desativar o Firewall para a rede, mas só deverá fazê-lo em casos específicos fundamentados.
- **Utilização compartilhada da conexão à Internet**: Em conexões diretas com a Internet, é possível definir se todos os computadores conectados através de uma ***rede TCP/IP*** devem ter acesso à Internet ou não. Essa ***liberação da conexão à Internet*** (***ICS***) pode ser geralmente ativada para uma rede doméstica.
- **Permitir configuração automática (DHCP)**: Na conexão do seu computador com a rede, é fornecido um ***Endereço IP dinâmico*** (através do ***DHCP*** = ***Dynamic Host Configuration Protocol (protocolo dinâmico de configuração de host)***). Se estiver conectado com a rede através dessa configuração padrão, deverá deixar a marcação.
- **Conjunto de regras**: Aqui você pode escolher rapidamente entre os conjuntos de regras pré-estruturados e definir, dessa forma, se trata-se p.ex., de uma rede confiável, não confiável ou a ser bloqueada em relação aos critérios de monitoramento do Firewall. Com o botão **Editar conjunto de regras** você tem também a possibilidade de configurar individualmente os conjuntos de regras. Para isto, leia também o capítulo **Conjunto de regras**.

Conjunto de regras

Nessa Área é possível criar regras especiais para diferentes redes. Essas regras são então respectivamente reunidas em um conjunto de regras. Os conjuntos de regras predefinidos são para ***conexão direta com a Internet***, ***redes não confiáveis***, ***redes confiáveis*** e ***redes a serem bloqueadas***. Na visualização geral, é exibido o respectivo conjunto de regras com o nome e status do modo furtivo. Com ajuda dos botões **Novo**, **Excluir** e **Editar** você pode alterar conjuntos de regras existentes ou adicionar novos.

? Com o ***Modo furtivo*** (oculto, escondido), as consultas ao computador que servem para verificar a acessibilidade das respetivas portas não são respondidas. Isso dificulta aos hackers a obtenção de informações sobre o sistema.

? Os conjuntos de regras predefinidos para ***conexão direta com a Internet***, ***redes confiáveis***, ***redes não confiáveis*** e ***redes a serem bloqueadas*** não podem ser excluídos. Conjuntos de regras adicionais criados por você podem naturalmente ser excluídos a qualquer momento.

Criar conjunto de regras

Você pode atribuir a cada rede um ***Conjunto de regras*** próprio (ou seja, uma coleção especial de regras definidas para isso). Dessa maneira, é possível proteger redes de forma diferente com níveis de risco diferenciados. Assim, uma rede doméstica privada precisa seguramente de menos proteção (e também trabalho de gerenciamento) do que uma de transmissão de dados remotos que está em contato direto com a Internet. O firewall contém três conjuntos de regras predefinidos para os seguintes tipos de rede:

- **Conjunto de regras para uma rede não confiável**: Aqui pertencem em geral, as redes abertas como p.ex., ***redes dial-up*** que têm acesso à ***Internet***.
- **Conjunto de regras para uma rede confiável**: Confiáveis são em geral as ***redes domésticas e empresariais***.
- **Conjunto de regras para uma rede a ser bloqueada**: Quando for necessário bloquear o contato de um computador a uma rede, por um período ou permanentemente, essa configuração pode ser utilizada. Isso é útil por exemplo, na conexão com ***Redes estranhas***redes estranhas, sobre as quais não se tem certeza sobre o padrão de segurança (p.ex. em ***LAN houses***, redes empresariais de estranhos, locais de trabalho abertos para notebooks e etc.).

Você pode atribuir um selecionado conjunto de regras correspondente para redes que acabam de ser estabelecidas no seu computador. Além disso, através do botão **Novo** é possível criar novos conjuntos de regras para redes. Para isso, clique na área de **Conjunto de regras** no botão **Novo** e defina na caixa de diálogo que aparece o seguinte:

- **Nome do conjunto de regras**: Insira aqui um nome significativo para o conjunto de regras.

- **Criar um conjunto de regras vazio**: Aqui você pode criar um conjunto de regras totalmente vazio e preenchê-lo exclusivamente com regras próprias.
- **Criar um conjunto de regras que contenha uma regra útil**: Nessa opção, você pode decidir se no novo conjunto de regras deverão ser definidas regras básicas para redes não confiáveis, confiáveis e redes a serem bloqueadas. Com base nessas predefinições, é possível então efetuar as alterações individuais.

O novo conjunto de regras aparecerá agora **na área de conjunto de regras**, abaixo do respectivo nome (p.ex.,***Novo conjunto de regras***) na lista. Se clicar agora em **Editar**, é aberto o **Assistente de regras** ou a **Caixa de diálogo avançada** para a edição das regras individuais desse conjunto de regras. Para saber como atribuir novas regras aos conjuntos de regras, leia os capítulos **Utilizar o Assistente de regras** ou **Utilizar a Caixa de diálogo avançada**.

> ? Além da inserção direta de regras, você tem também, naturalmente, a possibilidade de criar regras através da caixa de informações do Alarme do firewall. Este processo de aprendizado do Firewall é explicado no capítulo **Alarme do Firewall** .

Utilizar o Assistente de regras

Com o Assistente de regras você pode definir regras adicionais para o respectivo conjunto de regras ou alterar as regras existentes. Principalmente para usuários que não têm bons conhecimentos sobre a tecnologia de Firewall, recomendamos utilizar o ***Assistente de regras*** e não a ***Caixa de diálogo avançada***.

> ? Com o Assistente de regras você pode definir uma ou mais regras para o respectivo conjunto de regras selecionado. Ou seja, você cria sempre uma regra dentro de um conjunto de regras, que contém diversas regras.

> ? Dependendo do conjunto de regras definido para a respectiva rede, um aplicativo pode estar bloqueado em um conjunto de regras (p.ex., para redes não confiáveis) e na outra, ter total acesso à rede (p.ex. para redes confiáveis). Dessa forma, você pode, p.ex., restringir um navegador com diferentes regras correspondentes para que ele possa acessar páginas disponíveis em sua rede local, mas que não tenha nenhuma possibilidade de acessar conteúdo na rede de transmissão de dados remotos.

O Assistente de regras disponibiliza as seguintes regras básicas:

- **Permitir ou negar o acesso de um determinado aplicativo**: Através dessa opção é possível selecionar objetivamente um aplicativo (programa) no seu disco rígido e permitir ou proibir explicitamente o acesso à rede, definido através do conjunto de regras. Para isso, selecione no assistente, o programa desejado ***(Caminho do programa)*** e informe, em **Direção da conexão**, se o programa deve ser bloqueado para conexões de entrada, conexões de saída ou tanto para uma como para outra. Dessa forma, você pode, p.ex., impedir que o software do seu MP3 repasse dados sobre seus hábitos de áudio (conexão de saída) ou cuidar para que atualizações automáticas do produto sejam executadas (conexões de entrada).
- **Abrir ou bloquear um serviço da Internet específico (Porta)**: As ***Portas*** são áreas de endereço especiais que encaminham dados transmitidos através de uma rede automaticamente a um determinado Protocolo e com isso, a determinados softwares. Dessa forma é feita a transação da transmissão de sites comuns através da porta 80 por exemplo, o envio de e-mails através da porta 25, a captura de e-mails através da porta 10 e assim por diante. Sem o firewall, normalmente todas as portas do seu computador estão abertas, apesar de que a maioria não é necessária a usuários comuns. Através do bloqueio de uma ou mais portas é possível fechar brechas de segurança rapidamente, que podem, caso contrário, ser utilizadas por hackers para ataques. No assistente você tem a possibilidade de bloquear completamente as portas ou apenas para um aplicativo específico (p. ex., o seu software de reprodução de MP3).
- **Permitir ou negar compartilhamento de arquivos e impressora (NetBIOS)**: A ***NetBIOS*** é uma interface especial em redes e pode ser utilizada para efetuar a liberação de arquivos ou impressão diretamente de computador para computador sem utilizar para isso o protocolo TCP/IP. Como isso, na maioria das redes domésticas não é necessário, a NetBIOS pode ser usada por hackers para paralisar um computador; é aconselhável em muitos casos recusar essa liberação para redes não confiáveis.
- **Permitir ou negar serviços de domínio**: Um ***Domínio*** é um tipo de diretório estrutural para computadores em uma rede e permite com isso, uma administração centralizada dos computadores vinculados em uma rede. A liberação para serviços de domínio em redes não confiáveis deve ser recusada por via de regra.
- **Permitir utilização compartilhada da conexão à Internet**: Em conexões diretas com a Internet, é possível definir se todos os computadores conectados através de uma ***rede TCP/IP*** devem ter acesso à Internet ou não. Essa ***liberação da conexão à Internet*** (***ICS***) pode ser geralmente ativada para uma rede doméstica.

- **Alternar para o modo de edição avançado (caixa de diálogo avançada)**: Através dessa opção você pode alternar entre o Assistente de regras e a ***Caixa de diálogo avançada***. Informações sobre a Caixa de diálogo avançada podem ser encontradas no capítulo **Utilizar a Caixa de diálogo avançada**.

> **?** Se remover a marcação em **Iniciar o assistente de regras também no futuro**, o Firewall abrirá automaticamente a Caixa de diálogo avançada para as novas regras.

Utilizar a Caixa de diálogo avançada

Na caixa de diálogo avançada, você pode definir regras bastante individuais para a respectiva rede, contanto que tenha determinados conhecimentos sobre segurança de rede. Naturalmente, todas as regras podem ser criadas através do Assistente de regras, porém, configurações mais avançadas podem ser efetuadas. Para isso, as seguintes possibilidades estão disponíveis:

- **Nome**: Aqui é possível alterar, se necessário, o nome para o conjunto de regras atual. O conjunto de regras será exibido na lista na área **Conjunto de regras** e poderá ser combinado com as redes identificadas pelo Firewall.
- **Modo furtivo**: Com o modo furtivo (oculto, escondido), as consultas ao computador que servem para verificar a acessibilidade das respetivas portas não são respondidas. Isso dificulta aos hackers a obtenção de informações sobre o sistema.
- **Ação, caso nenhuma regra se aplique**: Aqui é possível definir se o acesso à rede deve ser em geral permitido, recusado ou regulado sob solicitação. Se outras regras forem definidas para programas individuais através da ***função autodidata*** do firewall, essas serão naturalmente consideradas.
- **Modo adaptativo**: O modo adaptativo auxilia você com os aplicativos que utilizam a chamada ***Tecnologia de canal reverso*** (p.ex., ***FTP*** e diversos ***jogos on-line***). Esse tipo de aplicativo conecta-se a um computador remoto e trata com ele um canal reverso, a partir do qual o computador remoto se "reconecta" a seu aplicativo. Se o modo adaptativo estiver ativo, o firewall reconhece esse canal reverso e permite o acesso sem consultar especificamente.

Regras

Na lista de regras, você pode encontrar todas as regras definidas como Exceções para esse conjunto de regras. Dessa forma, p.ex., é possível permitir aos programas selecionados Acessos à rede abrangentes, mesmo se a rede não tiver sido definida como confiável. As regras que entram aqui podem ter sido criadas de diferentes formas:

- Através do ***Assistente de regras***
- Diretamente através da ***Caixa de diálogo avançada*** através do botão **Novo**
- Através da caixa de diálogo na caixa de informações, que aparece em um alarme de firewall.

Naturalmente, cada conjunto de regras tem uma lista própria com regras.

> **?** Como as Regras do Firewall são estruturadas parcialmente de forma hierárquica, em alguns casos, é importante observar a ***classificação*** das regras. Assim, pode ocorrer que uma liberação de uma porta seja novamente bloqueada através da recusa do acesso a um protocolo. É possível alterar a seqüência da classificação de uma regra marcando-a com o mouse e movendo-a com a seta em **Classificação** para cima ou para baixo na lista.

Se você criar uma nova regra através da ***Caixa de diálogo avançada*** ou alterar uma regra existente através da ***Caixa de diálogo Editar***, aparece a caixa de diálogo **Editar regra** com as seguintes possibilidades de configuração:

- **Nome**: Aqui é encontrado, em regras predefinidas e geradas automaticamente, o ***nome do programa*** para o qual a respectiva regra se aplica. O nome pode ser alterado a qualquer momento ou informações complementares adicionadas através do botão **Editar**.
- **Regra ativa**: Uma regra pode ser desativada removendo a marcação sem ter que excluir a regra.
- **Comentário**: Aqui você obtém informações sobre como a regra foi gerada. Em regas predefinidas para o conjunto de regras é exibido **Regra predefinida** e, em regras que foram geradas a partir da caixa de diálogo do Alarme do Firewall é exibido **gerado por solicitação** e, para as regras geradas por você mesmo através da caixa de diálogo avançada, você pode inserir o seu próprio comentário.
- **Direção da conexão**: Com a ***direção***, é definido se isso refere-se a uma regra para conexões de entrada, de saída ou de entrada e saída para essa regra.

- **Acesso**: Aqui é definido se o acesso deve ser permitido ou negado dentro desse conjunto de regras para o respectivo programa.
- **Registro**: Aqui você pode selecionar que ***Registros de conexão*** você deseja permitir ou recusar para um acesso. Aqui, você tem a possibilidade de bloquear ou liberar protocolos em geral, ou acoplar a utilização do protocolo com o uso de um determinado ou de diversos aplicativos ***(Atribuir aplicativo)***. Da mesma forma, é possível definir exatamente as portas indesejadas ou desejadas através do botão **Atribuir serviço da Internet**.
- **Janela de tempo**: Você pode estruturar o acesso aos recursos da rede de forma dependente de tempo e, p.ex., cuidar para que um acesso só ocorra durante o seu horário de trabalho e não fora desse horário.
- **Espaço de end. IP**: Principalmente para redes com endereços IP fixo atribuídos, faz sentido regulamentar sua utilização através de uma restrição de espaço de endereço IP. Um espaço de endereço IP definido claramente, reduz significativamente o perigo de um ataque de hacker.

Alarme do Firewall

Em geral, o Firewall pergunta no modo **Criação manual de regras** se o acesso de programas e processos desconhecidos que querem se conectar à rede deve ser permitido ou recusado. Para isso, é aberta uma caixa de informações que fornece detalhes sobre o respectivo aplicativo. Aqui você tem a possibilidade de permitir ou recusar uma vez ou permanentemente o acesso à rede para o aplicativo. Assim que você permite ou recusa o acesso permanente a um programa, isso é registrado como ***regra*** no ***conjunto de regras*** das respectivas redes, e não será mais perguntado a partir desse momento. Os seguintes botões estão disponíveis para isso:

- **Permitir sempre**: Através desse botão você cria uma regra para os aplicativos listados acima (como ***Opera.exe***, ***Explorer.exe*** ou ***iTunes. exe***), que autoriza o acesso permanente à rede do aplicativo citado, como p.ex., à rede ou à Internet. Essa regra pode ser então encontrada como gerado por solicitação, na área **Conjunto de regras**.
- **Permitir temporariamente**: Através desse botão, você permite, ao respetivo aplicativo, um acesso único à rede. Na próxima tentativa de um acesso à rede por esse programa, o firewall irá novamente solicitar a permissão.
- **Recusar sempre**: Através desse botão você cria uma regra para os aplicativos listados acima (como ***dialer.exe***, ***spam.exe*** ou ***trojan.exe***), que autoriza ou recusa o acesso permanente à rede pelo aplicativo citado, como p.ex., à rede ou à Internet. Essa regra pode ser então encontrada como gerado por solicitação, na área **Conjunto de regras**.

- **Recusar temporariamente**: Através desse botão, você proíbe, ao respectivo aplicativo, um acesso único à rede. Na próxima tentativa de um acesso à rede por esse programa, o firewall irá novamente solicitar a permissão.

Outras informações sobre ***Protocolo***, ***Porta*** e ***Endereço IP*** podem ser obtidas no próprio aplicativo com o qual você deseja interagir.

Registro

Na Área de registros são registradas todas as conexões com a rede e Internet permitidas e bloqueadas pelo Firewall. Essa lista pode ser organizada da forma desejada, clicando nos respectivos títulos das colunas e clicando no botão **Detalhes**, para obter mais informações sobre cada conexão.

Opções - Firewall

Na barra de menu superior da interface do programa, você encontra através do clique no botão **Opções** funções e possibilidades de configuração abrangentes.

Automático

Aqui é possível optar pelo Modo Piloto automático e a Criação manual de regras:

Modo Piloto automático (recomendado): Aqui o Firewall trabalha de forma totalmente autônoma e evita os perigos automaticamente de PCs residenciais. Essa configuração oferece uma proteção geral prática e é, na maioria dos casos, recomendável.

Criação manual de regras: Se desejar configurar o seu Firewall de forma individual ou não desejar que determinados aplicativos não trabalhem junto com o Piloto automático, poderá ajustar a sua proteção de Firewall através da criação manual de regras totalmente às suas necessidades pessoais.

Anexo

Resolução de problemas (FAQ)

Nesta área, você encontra respostas a perguntas que podem possivelmente ocorrer no trabalho com o *G Data Software*.

Eu desejo executar a instalação do cliente de forma central, a partir do servidor, através do Administrator

A forma mais confortável é a ***instalação através do Administrator***. Para isso, os clientes precisam atender a determinadas condições. A ***Instalação remota*** pode ser executada de duas formas. Quando o cliente atende os pré-requisitos, os arquivos são copiados diretamente e os registros são inseridos no registry. Se o servidor só puder acessar o disco rígido, mas não o registry ou outros requisitos do sistema não forem atendidos, o programa de instalação completo é copiado no cliente e iniciado na próxima inicialização do computador automaticamente. Para a instalação, vá para a barra de menu do vorgenommen e abra, de lá, a função ***Cliente > Instalar o G Data Client***. Uma janela para entrada de dados aparece, na qual você insere nome de usuário, senha e domínio do ManagementServer. Após a inserção desses dados, aparece uma janela com todos os computadores disponíveis na rede. Os clientes ativados são marcados com um ícone. Os clientes desativados são apresentados por um ícone sombreado. Para a instalação, selecione um computador da rede e clique, em seguida, no botão **Instalar**. Dessa forma, o *G Data Client* é instalado nesse computador. Se o seu sistema não atender aos requisitos para uma instalação remota do *software G Data Client*, você tem, naturalmente, também a possibilidade de instalar no cliente de forma manual ou semiautomática, o *software G Data Client*.

Eu desejo instalar o Administrator em um computador cliente

O ***Administrator*** pode naturalmente ser iniciado a partir de qualquer outro computador na rede.

? Para um andamento sem problemas do *G Data Software* , não é necessário instalar o Administrator nos clientes. Uma instalação do Administrator em um computador cliente, é recomendada somente em caso de necessidade para solução de um problema *no local*.

Para isso, recomendamos liberar o diretório ***Admin*** e abrir o arquivo ***Admin.exe*** nos outros computadores. Naturalmente o arquivo pode também ser copiado em outros computadores e, lá, iniciado. A liberação tem a vantagem de que sempre a versão mais recente será instalada, porque o arquivo pode ser atualizado através de uma atualização na Internet. Opcionalmente é possível, por isso, colocar o *CD-ROM G Data* na unidade de CD-ROM do computador cliente, pressionar o botão **Instalar** e, em seguida, selecionar o componente *G Data Administrator* através de um clique no respectivo botão. Na tela de saudação a seguir, você é informado que está prestes a instalar o Administrator em seu sistema. Feche, o mais tardar agora, todos os aplicativos abertos em seu sistema Windows, porque esses poderão causar problemas na instalação. Clique em **Continuar**, para proceder com a instalação. A tela seguinte possibilita a seleção do local no qual os dados do Administrator deverão ser salvos. Por padrão, o ManagementServer é salvo em ***C: > Programas > G Data > G Data Administrator***. Se desejar selecionar um outro local de armazenamento, você tem a possibilidade de, através do botão **procurar**, abrir uma visualização de diretório, na qual você pode selecionar um outro diretório, ou criar um novo. Com **Continuar**, você acessa a próxima etapa de instalação. Agora você tem a possibilidade de selecionar um grupo de programas. Se clicar em**Continuar**, encontrará o programa, por padrão, no grupo de programas ***G Data Administrator***, na seleção de programas do menu Iniciar do Windows. A instalação será concluída com uma tela de conclusão. Clique em **Finalizar**. O Administrator estará agora à sua disposição. A ferramenta Administrator pode ser aberta para controle do ManagementServers com um clique no registro ***G Data Administrator*** no grupo de programas ***Iniciar > (Todos os) Programas > G Data ManagementServer*** no menu Iniciar.

Eu desejo equipar os clientes com a ajuda do CD-ROM G Data, com o software cliente

O software cliente pode também ser diretamente instalado nos clientes individuais com o CD fornecido. Para isso, insira o ***CD-ROM*** na unidade de CD-ROM do computador cliente, selecione o componente ***G Data Client*** com um clique no botão ao lado. Na instalação, você será solicitado a informar o nome do computador no qual o ManagementServer está instalado. Informe o nome correspondente (p.ex. ***avk_server***). Pressionando o botão **Continuar**, você conclui a instalação. Se o programa de instalação na tela de conclusão sugerir a reinicialização do computador, execute-a, porque o cliente, neste caso, só estará funcional após uma reinicialização.

Alguns clientes avisam "O banco de dados de vírus está corrompido". O que deve ser feito?

Para garantir uma proteção ideal contra vírus, o banco de dados de vírus é regularmente verificado quanto a sua integridade. Em caso de erro, o relatório ***O banco de dados de vírus está corrompido.*** é adicionado. Exclua o relatório e carregue a atualização corrente do banco de dados de vírus de nosso servidor. Em seguida, execute uma atualização do banco de dados de vírus do cliente afetado. Entre em contato com o nosso suporte quando o relatório de erro for novamente adicionado.

Os clientes não devem ser tratados através de seus nomes, mas através de seus endereços IP.

Instalação do ManagementServer: Na instalação, será solicitado pelo nome do servidor. O nome deve ser substituído pelo ***Endereço IP***. O nome do servidor poderá também ser substituído pelo endereço IP quando o ManagementServer já estiver instalado. Para isso, adapte o registro no Registry

HKEY_LOCAL_MACHINE\Software\G Data\G Data ManagementServer\ComputerName

e o arquivo

\Programas\G Data\G Data ManagementServer\AvkClientSetup\RegServer.txt

. ***Ativação do cliente no Administrator***: Para que a conexão do servidor para os clientes possa ser estabelecida também através do endereço IP, os clientes precisam ser ativados no Administrator com seu endereço IP.

Isso pode ser feito manualmente (***Ativar cliente/clientes (Diálogo)***) ou procurando por um endereço IP (***Procurar computador/cliente***).
Instalação do G Data Client a partir do CD: Quando os clientes forem instalados a partir do ***CD***, o programa de instalação pergunta pelo nome do servidor e pelo nome do computador. Informe aqui, respetivamente, o endereço IP.

Minha caixa postal foi movida para a quarentena

Isso pode ocorrer quando um e-mail infectado estiver na caixa postal.
Mover de volta o arquivo: Feche o programa de e-mail no cliente afetado e exclua, eventualmente, um arquivo compactado recém-criado. Em seguida, abra, com o Administrator, o relatório correspondente e clique em ***Restaurar arquivo***. Entre em contato com nosso suporte se a restauração falhar.

Como posso verificar se os clientes têm uma conexão com o ManagementServer?

A coluna **Último acesso** na área de tarefas **Clients** contém o momento no qual o cliente conectou-se pela última vez no ManagementServer. Normalmente os clientes comunicam-se a cada alguns minutos com o ManagementServer (quando nenhuma tarefa de verificação estiver sendo realizada no momento). As seguintes razões podem ser a causa de uma conexão mal-sucedida.

- O cliente está desativado ou desconectado da rede.
- Nenhuma conexão TCP/IP pode ser estabelecida entre o cliente e o ManagementServer. Verifique as configurações de rede.
- O cliente não pode determinar o endereço IP do servidor, ou seja, a resolução de nome não funciona. A conexão pode ser verificada com o comando ***ping***. Para isso, no prompt, dê o comando ***ping <nome do servidor>***, onde ***<nome do servidor>*** é o nome do computador da rede no qual o ManagementServer está instalado.

Alguns clientes avisam "Os arquivos de programa foram alterados ou estão danificados". O que deve ser feito?

Para garantir uma proteção ideal contra vírus, os arquivos de programa são regularmente verificados quanto a sua integridade. Em caso de erro, o relatório ***Os arquivos de programa foram alterados ou estão danificados*** é adicionado. Exclua o relatório e carregue a atualização corrente dos arquivos de programa (*G Data Client*) de nosso servidor. Em seguida, execute uma atualização dos arquivos de programa do cliente afetado. Entre em contato com o nosso suporte quando o relatório de erro for novamente adicionado.

Após a instalação do cliente, alguns aplicativos funcionam bem mais lentos do que antes

A sentinela verifica, em segundo plano, todos os acessos a arquivos, além de verificar os arquivos abertos e armazenados em relação a vírus. Isso leva a um ***retardo***, normalmente, praticamente não percebido. Caso um aplicativo abra muitos arquivos ou alguns arquivos com muita frequência, pode ocorrer um retardo substancial. Para lidar com esse problema, desative primeiro temporariamente a sentinela para descobrir se é ela mesma a causadora dos retardos. Quando o computador afetado acessa arquivos de um servidor, naturalmente, a sentinela precisa também ser desativada. Caso a sentinela seja a causa, o problema pode ser resolvido, através da definição de uma ***Exceção*** (= arquivos que não deverão ser verificados). Para isso, primeiro os arquivos, aos quais o acesso é constante, precisam ser determinados. Com um programa como o ***MonActivity***, esses arquivos podem ser determinados. Se necessário, entre em contato com nosso***Suporte técnico***. Retardos conhecidos:

- Na utilização de algumas ***impressoras HP*** com o ***Microsoft Office*** , os arquivos ***HP*.INI*** devem ser definidos como exceção.
- Na utilização do software de e-mail ***Eudora***, os arquivos ***EUDORA.INI*** e ***DEUDORA.INI*** devem ser definidos como exceção.

? Naturalmente o desempenho pode ser melhorado, através da não utilização de ambos os mecanismos de verificação de vírus e usando apenas um.

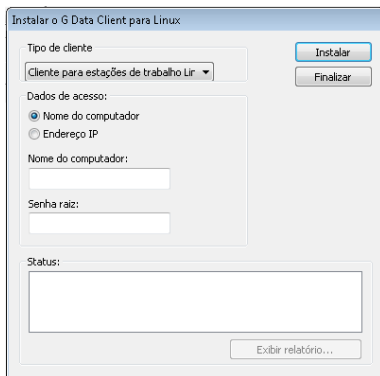
Leia para isso o capítulo Software cliente em computadores Linux

O produto possibilita utilizar a ***proteção antivírus G Data*** em ***estações de trabalho Linux*** de diferentes distribuições. O ***cliente Linux*** pode, nesse processo (assim como os ***clientes Windows***), ser vinculado à infraestrutura do *G Data ManagementServer* e controlado de forma central através do *software G Data Administrator* e ser fornecido com atualizações de assinaturas. De forma análoga aos clientes do Windows, nos clientes Linux, é criada uma sentinela dos sistema de arquivos com uma interface de usuário que se orienta na funcionalidade da versão Windows. Para computadores Linux que funcionam como ***Servidor de arquivos*** e disponibilizam liberações do Windows aos diversos clientes (através do ***protocolo SMB***), pode ser instalado um módulo que controla o acesso às liberações e executa uma verificação no arquivo a cada acesso, de forma que nenhum malware de servidor Samba possa acessar os clientes Windows (e vice-versa).

? Para o ***cliente da estação de trabalho***, uma versão do Kernle superior ou igual à 2.6.25 é necessária, isso é o caso do Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11 e outras distribuições atuais. Para outras distribuições, é necessário, em casos inidviduais, uma adaptação. O ***cliente do servidor de arquivos*** pode ser utilizado em todas as distribuições comuns.

Para instalar o sofwtare no cliente Linux, proceda da seguinte forma:

1 ***Instalação remota do software cliente através da rede***

Na área de tarefas**Clientes** , no menu **Configurações do cliente** , selecione o comando **Instalar o G Data Client para Linux**. Uma janela de diálogo será aberta, através da qual será possível definir o cliente no qual o software cliente deverá ser copiado. Para isso, o computador deverá ser conhecido na rede.

2 Utilize a opção **Nome do computador**, quando no computador cliente um ***serviço Samba*** tiver sido instalado ou quando o computador estiver registrado no ***Servidor de nomes*** da rede. Se o nome do computador não for conhecido, utilizar o **Endereço IP** do computador.

3 Insira agora a **Senha raiz** do computador. Para uma instalação remota, é preciso que uma senha raiz tenha sido concedida. Por padrão, em algumas distribuições, p.ex., a Ubuntu, esse não é o caso.

4 Clique agora no botão **Instalar**. Na área **Status** , você vê se a instalação do software cliente foi bem-sucedida.

? ***Instalação manual do software cliente***

Em um diretório especial no CD do programa, você encontra os seguintes arquivos

- **installersmb.bin** = Instalador para servidor de arquivos Samba
- **installerws.bin** = Instalador para estação de trabalho

Esses arquivos podem ser copiados no computador cliente e iniciar o arquivo correspondente para a instalação do software cliente.

Além disso, aqui você encontra um outro arquivo com as ***Assinaturas de vírus***. Como o software, após a instalação, recupera as assinaturas de vírus mais recentes do servidor, a instalação desse arquivo é facultativa:

- **signatures.tar** = Pasta compactada com assinaturas de vírus

Clientes do servidor de arquivos Linux: Nenhuma conexão será estabelecida ao ManagementServer/ as assinaturas não serão atualizadas

1 Verifique se ambos os processos do *G Data Client* estão em execução: Insira na linha de comando

linux:~# ps ax|grep av

. Você deverá receber

...   Ssl   0:07 /usr/sbin/avkserver --daemon

...   Ssl   0:05 /usr/sbin/avguard --daemon

como resultado. Independente da distribuição utilizada, você pode iniciar os processos com

linux:~# /etc/init.d/avkserver start

linux:~# /etc/init.d/avclient start

e com

linux:~# /etc/init.d/avkserver stop

linux:~# /etc/init.d/avclient stop

interrompê-los. Aqui é preciso estar logado como administrador (=“root“) no computador Linux.

2 Os arquivos de registro podem ser vistos em: Abaixo de ***/var/log/avk*** encontram-se os arquivos de registro ***avk.log*** e ***remote.log***. No arquivo ***avk.log***, são registrados os resultados do verificador ***avkserver***; no arquivo***remote.log***, encontram-se os resultados do processo ***avclient***, que estabelece a conexão com o *G Data ManagementServer*. Dê uma olhada nos arquivos e procure por mensagens de erro. Se desejar ver mais mensagens, você pode colocar, nos arquivos de configuração ***/etc/gdata/gdav.ini*** e ***etc/gdata/avclient.cfg***, os registros para ***Loglevel*** para o valor ***7***.

Cuidado: Níveis de registro altos criam muitas mensagens e fazem com que os arquivos de registro cresçam rapidamente. No funcionamento normal, defina o Nível de registro sempre para valores mais baixos!

3. Teste o verificador: Com a ferramenta de linha de comando ***avkclient***, você pode testar a função do servidor de varredura ***avkserver***. Os seguintes comandos podem ser executados:

   linux:~$ avkclient avkversion - informa versão e data de atualização das assinaturas de vírus

   linux:~$ avkclient version - informa versão abreviada

   linux:~$ avkclient scan:<file> - varre o arquivo ***<file>*** e dá o resultado

4. Os arquivos de configuração podem ser vistos em: Em ***etc/gdata/avclient.cfg***, você encontra os arquivos de configuração do cliente remoto ***avclient***. Controle se o endereço do servidor de gerenciamento principal (MainMMS) está inserido corretamente. Caso não esteja, exclua o falso registro e faça novamente o login do cliente Linux através do *G Data Administrator* ou insira diretamente o endereço do *G Data ManagementServer*.

5. Teste suas liberações: A proteção de vírus para a liberação do Samba é ativada através do registro

   vfs objects = gdvfs

   no arquivo de configuração do Samba ***/etc/samba/smb.conf***. Se o registro estiver na seção ***[global]***, a proteção é ativada para todas as liberações. Se a linha estiver em uma outra seção, a proteção vale somente para a respetiva liberação. A linha pode ser comentada (colocando um jogo da velha (#) para determinar se o acesso funciona sem a proteção antivírus. Caso não, procure primeiro pelo erro na configuração do seu Samba.

6. ***Sentinela da estação de Trabalho Linux***

   Verifique se o processo da sentinela ***avguard*** está em execução:

   ps ax|grep avguard

   A sentinela precisa do módulo Kernel ***redirfs*** e ***avflt***. Com ***lsmod***, é possível verificar se os módulos estão carregados: ***lsmod|grep redirfs*** e ***lsmod| grep avflt***....

   Os módulos precisam estar compilados para o Kernel utilizado por você. Isso resolve o ***Dynamic Kernel Module System*** (***DKMS***), o qual deverá estar instalado com os pacotes de cabeçalho do Kernel adequados, à sua distribuição. Quando for esse o caso, o DKMS compila e instala os módulos automaticamente. O ***arquivo de registro*** da sentinela pode ser encontrado em ***/var/log/gdata/avguard.log***.

Acordo de licença

A seguir estão relacionadas as condições contratuais para a utilização do *Software* ***G Data EndpointProtection*** pelo usuário final (doravante também: proprietário da licença).

1. Objeto do contrato: O objeto do contrato é o *G Data Software* e a descrição do programa, gravados em uma mídia de dados ou a partir de download da Internet. Doravante chamados também de Software. A *G Data* ressalta que, de acordo com a situação tecnológica atual, não é possível criar softwares que funcionem corretamente em todos os aplicativos e combinações.

2. Escopo da utilização: A *G Data* concede o direito simples, não exclusivo e pessoal (doravante chamado também de Licença), pela duração deste contrato de utilização do software na quantidade de computadores acordada contratualmente. A utilização do software pode ocorrer na forma de uma instalação em uma unidade física (CPU), uma máquina virtual/emulada (como VMWare) ou uma instância de uma sessão de terminal. Se esse computador for também um sistema multi-usuário, esse direito de utilização vale para todos os usuários de um sistema. Como proprietário da licença, você pode transferir o software de forma física (ou seja, armazenado em uma mídia de dados) de um computador a outro, contanto que seja em algum momento, utilizado na quantidade de computadores acordada contratualmente. Não é permitida a utilização mais abrangente.

3. Restrições especiais: É proibido ao proprietário da licença alterar o software sem a prévia permissão por escrito da *G Data*.

4. Propriedade de direitos: Com a aquisição do produto você recebe apenas a propriedade da mídia de dados física, onde o software está gravado e as atualizações acordadas no escopo do suporte. Não existe vinculação da aquisição de direitos ao software. A *G Data* se reserva principalmente todos os direitos de publicação, multiplicação, processamento e utilização do software.

5. Multiplicação: O software e a respectiva documentação são protegidos pela lei de direitos autorais. É permitida a criação de uma cópia de segurança que, no entanto, não pode ser repassada a terceiros.

6. Duração do contrato: O contrato tem duração indeterminada. Esse tempo de duração não abrange o fornecimento de atualizações. O direito do proprietário da licença para utilização do software expira automaticamente e sem aviso prévio, quando esse violar uma das condições deste contrato. No encerramento do direito de utilização, o proprietário da licença é obrigado a destruir o CD-ROM original, inclusive todas as ATUALIZAÇÕES/UPGRADES, assim como a documentação escrita.

7. Restituição por danos em caso de violação do contrato: A *G Data* ressalta que, você, o proprietário da licença, é o responsável por todos os danos que possam incorrer à *G Data* devido à violações de direitos autorais e resultantes de violações das determinações deste contrato.

8. Alterações e atualizações: Respectivamente, são válidas nossas condições de serviço atuais. As condições de serviço podem ser alteradas a qualquer momento sem aviso prévio e, sem a necessidade de informação sobre os motivos.

9. Garantia e responsabilidade da *G Data*:

a) A*G Data* garante ao proprietário original da licença que, no momento da entrega do software, a eventual existência da mídia de dados (CD-ROM) onde o software foi gravado está livre de erros de execução de material, sob condições operacionais e manutenção normais.

b) Se a mídia de dados ou o download da Internet estiverem defeituosos, o comprador pode solicitar a reposição durante o tempo da garantia de 6 meses após a entrega. Para isso, a compra do software deverá ser comprovada.

c) De acordo com as razões acima citadas no item 1, a *G Data* não assume nenhuma responsabilidade pelo total funcionamento do software. Em particular, a *G Data* não assume qualquer garantia de que o software atenda às demandas e finalidades do comprador ou que funcione em compatibilidade com outros programas adquiridos. É do comprador a responsabilidade pela escolha correta e as conseqüências da utilização do software, assim como os resultados intencionados ou obtidos. O mesmo vale para a documentação escrita que acompanha o software. Se o software não estiver utilizável dentro do escopo citado no item 1, o comprador tem o direito de desfazer o contrato. A *G Data,* tem o mesmo direito, dentro do escopo citado no item 1, quando a fabricação não for possível dentro de um esforço razoável.

d) A *G Data* não é responsável por danos, a não ser que o dano tenha sido causado intencionalmente ou por negligência culpável da *G Data*. A responsabilidade por negligência culpável é excluída em relação aos comerciantes. A responsabilidade de restituição máxima corresponde ao valor de compra do software.

10. Fóro: O fóro único para dirimir todos os conflitos resultantes direta ou indiretamente é, de acordo com a nossa escolha, o local da sede da *G Data*.

11. Determinações finais: Se alguma disposição deste acordo de licença for inválida, permanecerão as restantes em vigor. Como substituta da determinação inválida, valerá como acordado, uma determinação em vigor que seja mais parecida para o devido fim.

?

[G Data EndpointProtection - 28.09.2010, 10:19]

Índice

A

B

C

V

W